Chinese Cyber Economic Espionage: Motivations and Responses

A Monograph

by

LtCol G. Todd Puntney
USMC

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

2016

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
27-04-2016	SAMS Monograph	

4. TITLE AND SUBTITLE
Chinese Cyber Economic Espionage: Motivations and Responses

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
LtCol G. Todd Puntney, USMC

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
School of Advanced Military Studies (SAMS)
201 Reynolds Avenue
Fort Leavenworth, KS 66027-2134

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Command and General Staff College
731 McClellan Avenue
Fort Leavenworth, KS 66027-1350

10. SPONSOR/MONITOR'S ACRONYM(S)
CGSC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Alleged Chinese cyber economic espionage periodically fills headlines, Internet security company reports, Congressional hearing transcripts, and official (and semi-official) pronouncements. Despite the apparent recognition of a problem, the United States has been seemingly ineffective in deterring or dissuading continued Chinese cyber activity—despite the potential significant impact to economic and national security. While accurate calculations on the cost of stolen intellectual property to US businesses are nearly impossible to determine, some estimates suggest hundreds of billions of dollars per year—independent of broader and more sinister implications for the future of US competitiveness. Why China, apparently, believes it must steal at the expense of the United States, and why the United States has been unable to stem it, are crucial national security questions. An analysis of China's strategic ambitions, coupled with national policies designed to achieve them, illuminate possible answers. Similarly, an examination of the US response during the Obama Administration highlights the interplay between policy development and the influence of domestic politics, corporate interests, and narratives.

15. SUBJECT TERMS
China, cyberspace, economic espionage, Obama Administration, cyberspace policy.

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			LtCol G. Todd Puntney
Unclassified	Unclassified	Unclassified		62	**19b. TELEPHONE NUMBER** *(include area code)* 540-419-0602

Monograph Approval Page

Name of Candidate: LtCol G. Todd Puntney

Monograph Title: Chinese Cyber Economic Espionage: Motivations and Responses

Approved by:

_____, Monograph Director
Christopher Marsh, PhD

_____, Seminar Leader
William J. Gregor, PhD

_____, Director, School of Advanced Military Studies
Henry A. Arnold III, COL, IN

Accepted this 26th day of May 2016 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, PhD

Abstract

Chinese Cyber Economic Espionage: Motivations and Responses, by LtCol G. Todd Puntney, 55 pages

Alleged Chinese cyber economic espionage periodically fills headlines, Internet security company reports, Congressional hearing transcripts, and official (and semi-official) pronouncements. Despite the apparent recognition of a problem, the US has been seemingly ineffective in deterring or dissuading continued Chinese cyber activity—despite the potential significant impact to economic and national security. While accurate calculations on the cost of stolen intellectual property to US businesses are nearly impossible to determine, some estimates suggest hundreds of billions of dollars per year—independent of broader and more sinister implications for the future of US competitiveness. Why China, apparently, believes it must steal at the expense of the United States, and why the United States has been unable to stem it, are crucial national security questions. An analysis of China's strategic ambitions, coupled with national policies designed to achieve them, illuminate possible answers. Similarly, an examination of the US response during the Obama Administration highlights the interplay between policy development and the influence of domestic politics, corporate interests, and narratives.

Contents

Acronyms

APT	Advanced Persistent Threat
CCP	Chinese Communist Party
DHS	Department of Homeland Security
DOD	Department of Defense
FBI	Federal Bureau of Investigation
IP	Intellectual Property
IT	Information Technology
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OPM	Office of Personnel Management
PLA	People’s Liberation Army
RAT	Remote Access Tool

Introduction

> This world—cyberspace—is a world that we depend on every single day... [it] has made us more interconnected than at any time in human history.
>
> —President Obama; epigraph to Chapter I of the International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (May 2011)

> We count on computer networks to deliver our oil and gas, our power and our water. We rely on them for public transportation and air traffic control… But just as we failed in the past to invest in our physical infrastructure—our roads, our bridges and rails—we've failed to invest in the security of our digital infrastructure… This status quo is no longer acceptable—not when there's so much at stake. We can and we must do better.
>
> —President Obama; epigraph to White House Fact Sheet: Cybersecurity Legislative Proposal (May 12, 2011)

> From now on, our digital infrastructure—the networks and computers we depend on every day—will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority.
>
> —President Obama; epigraph to White House Fact Sheet: The Administration's Cybersecurity Accomplishments (May 12, 2011)

That the White House would append three epigraphs to three documents relating to cyberspace policy is understandable. In the world of narratives and spin, epigraphs provide connective tissue to demonstrate consistency and issue validity. Yet in this instance, the epigraphs all stemmed from the same presidential speech given two years before.[1] While plucking quotes across such a politically vast temporal expanse might suggest sagacity and the accuracy of long-range planning, perhaps the epigraphs owe their existence less to consistency and more to lost opportunity. Had the Obama Administration done more between May 2009 and May 2011, presumably staff authors could have harvested from different source material had there been more fertile policy ground.

[1] White House, Office of the Press Secretary, *Remarks by the President on Securing Our Nation's Cyber Infrastructure*, May 29, 2009, accessed January 10, 2016, https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

For the strategically compelling issue of cyberspace and Chinese economic espionage, the administration similarly seemed to wander. One of the most significant proclamations designed to inform the public about an alleged nexus between America's rising competitor and the widespread theft of corporate secrets came not from the government but instead, three years into the president's first term, from retired government officials (who, admittedly, were likely acting as proxies). In a January 2012 editorial in the *Wall Street Journal*, Vice Admiral (ret.) Mike McConnell (former Director of National Intelligence as well as Director of the National Security Agency), Michael Chertoff (former Secretary of the Department of Homeland Security), and William Lynn (former Deputy Secretary of Defense) were clear: "The Chinese government has a national policy of economic espionage in cyberspace. In fact, the Chinese are the world's most active and persistent practitioners of cyber espionage today."[2] The cost to the United States—in terms of competitiveness, innovation, dollars, and jobs—is "potentially catastrophic."[3]

At a 2015 speech at the University of Missouri, McConnell was more forceful. "About 80% of economic espionage, today, is conducted by the Chinese…The Chinese have penetrated every major corporation, of any consequence, in the United States."[4] The intent, he said, was an extension of a plan developed in the 1980s to regain national prominence through acquisition of technology and know-how. Whereas the Chinese first relied upon students flooding American universities to bring skills back to China, then later upon extracting foreign technology from Western companies through joint ventures, now China—with perhaps 100,000 hackers in the

[2] Mike McConnell, Michael Chertoff, and William Lynn, "China's Cyber Thievery is National Policy, and it Must be Challenged," *Wall Street Journal*, January 27, 2012, accessed October 2, 2015, http://www.wsj.com/articles/SB10001424052970203718504577178832338032176.

[3] Ibid.

[4] Mike McConnell, untitled speech (video of lecture, Bond Lecture Series, University of Missouri, March 12, 2015), accessed January 8, 2016, https://www.youtube.com/watch?v =_RPT9pAVUsY.

People's Liberation Army (PLA) and an equal number of civilians—could steal the information for free, "at the terabit level."[5]

The 2014 US indictment of five PLA officers for cyber economic espionage is a snapshot. While the alleged cyberspying, in this instance, was largely limited to nuclear energy, solar panels, and the steel industry, it illustrates what, precisely, China is looking for: technical specifications and blueprints, manufacturing techniques and processes, company financial and management details—all to gain a competitive advantage over the United States. [6]

According to a 2011 report from the Office of the National Counterintelligence Executive, calculating the true cost of the theft of American intellectual property, independent of who stole it or how, is exceedingly difficult.[7] The Commission on the Theft of American Intellectual Property (IP Commission)—a private, independent panel co-chaired by retired Admiral Dennis Blair and former Ambassador Jon Huntsman—attempted to portray, in a 2013 report, the scale of the damage: more than $300 billion per year, the loss of millions of jobs, and the erosion of American innovative spirit.[8] While neither report could pinpoint the true extent of Chinese theft through cyberspace, both were highly suggestive: "Chinese actors are the world's

[5] McConnell, untitled speech.

[6] Jose Pagliery, "What were China's Hacker Spies After?," CNNMoney, May 19, 2014, accessed January 8, 2016, http://money.cnn.com/2014/05/19/technology/security/china-hackers/?iid=EL.

[7] Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011* (Washington, DC: October 2011): i, 3, accessed December 5, 2015, https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf. For instance, corporations may not know, or disclose, that their secrets have been stolen, thus leaving costs hidden. As well, costs can be calculated on different bases, such as sunk costs of past research and development or opportunity costs of lost future business potential. Some costs, such as business plans or negotiating strategies, cannot be objectively determined.

[8] Commission on the Theft of American Intellectual Property, *The IP Commission Report* (n.p.: National Bureau of Asian Research, May 2013), 2, 27, accessed December 5, 2015, http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

most active and persistent perpetrators of economic espionage,"[9] accounting for 50-80% of the theft and using "especially pernicious" cyber methods[10] to exploit an increasingly connected world.

If China is the most active purloiner of American intellectual property, and if cyber economic espionage is, according to former Director of the National Security Agency (NSA) General Keith Alexander, the "greatest transfer of wealth in history,"[11] then the biggest thief may soon possess the biggest economy.

The questions become apparent: Why does China want the largest economy? Why does it have to cheat to get there? And why hasn't the United States been able to stop it?

An analysis of China's strategic ambitions, coupled with national policies designed to achieve them, illuminate possible answers: a nation yearning to reassert its position as a regional and global power—and a government concerned above all with social stability to preserve its rule—depends upon an economy that is globally competitive and continuously expanding. That such an imperative would emerge at the same time as the Internet transformed the social, economic, and political dimensions of human interaction provides novel opportunity. While certainly economic espionage has existed for centuries, the Internet—designed for the free flow of information and not its security—has dramatically improved its potential.

At the same time, an examination of how the United States has responded provides additional insights. Because cyber-enabled economic espionage has as its distinguishing feature cyberspace, which is neither exclusively public nor private, responses span political and social

[9] Office of the National Counterintelligence Executive, i.

[10] Commission on the Theft of American Intellectual Property, 3, 18.

[11] John Rogin, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History'," *Foreign Policy*, July 9, 2012, accessed August 12, 2015, http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/?wp_login_redirect=0).

levels and are generally within the broader context of cybersecurity. Given that much of the publicly available debate of Chinese cyber economic espionage has occurred since President Obama assumed office, the chronology of government action between 2009-2015 highlights an incremental approach filled with tension. Recognizing the limits of executive action, particularly since economic espionage targets the private sector, the administration has sought legislation that would better enable cooperation between the government and businesses. Yet domestic politics, corporate interests, and a meandering narrative likely inhibited policies that would both improve US cybersecurity (and therefore defense against cyber economic espionage) and change Chinese behavior.

Chinese motivations

That China has risen—and continues to rise—is without question. Divining its strategic intentions, however, now that it has arrived, is problematic. At a 2012 speech, after becoming the General Secretary of the Communist Party of China, Xi Jinping offered his vision of the future. "In my view, to realize the great renewal of the Chinese nation is the greatest dream for the Chinese nation."[12] As initially expressed by Xi (and further institutionalized since),[13] the "China Dream" aims to harness the power of the Party and people for the "great rejuvenation."[14]

Henry Kissinger, in *World Order*, offers insights into such a national revival. Tracing China's history—from its role as the enlightened center of the world; to its "century of humiliation" as it succumbed to the colonial ambitions of the West and Japan; to its Communist

[12] Xinhua News Agency, "Xi Pledges 'Great Renewal of Chinese Nation'," Xinhuanet, November 29, 2012, accessed April 1, 2016, http://news.xinhuanet.com/english/china/2012-11/29/c_132008231.htm.

[13] Benjamin Carlson, "The World According to Xi Jinping," *The Atlantic*, September 21, 2015, accessed April 1, 2016, http://www.theatlantic.com/international/archive/2015/09/xi-jinping-china-book-chinese-dream/406387/#article-comments.

[14] Xinhua News Agency, "Xi Pledges."

birth under a Mao who sought to restore China but nearly destroyed it in the process; to its rebirth under Deng who ushered in reforms that enabled its rise—Kissinger concludes that its return to "eminence in the twenty-first century is not new, but reestablishes historic patterns."[15] The prevailing international and economic conditions that fostered its restoration, however, distinguish its self-view today from its historical antecedents. Instead of finding itself as the benevolent empire owed fealty or eschewing the Cold War international order by isolating itself from it, China, since 1978, has embraced the international system. Which points to the challenge of how an aspiring China evolves in a global order with predefined rules largely enforced by a hegemon, without risking war to achieve it.

Avery Goldstein suggests that, given an anarchic international order, nation states are confronted with a security dilemma, "the difficult choice between taking steps to cope with possible dangers (which may provoke a rival to respond in kind) and exercising restraint (which may leave one more vulnerable than necessary if a potential rival does not reciprocate)."[16] For China, that means rising peacefully in a US-dominated international order and balancing pursuit of national interests with the realities of the strategic environment, yet with the potential risk of a US response designed to counter its ascent. Zhu Feng contends that, given such constraints, "in the present unipolar system, China is a satisfied, cooperative, and peaceful country."[17] At the same time, though, China sees the United States as the "most dangerous challenge not only to China's sovereignty claims and territorial integrity but also to the legitimacy of the Communist Party's rule and the survival of its political institutions."[18] If China views the United States as its

[15] Henry Kissinger, *World Order* (New York: Penguin Press, 2014), 220.

[16] Avery Goldstein, "Parsing China's Rise: International Circumstances and National Attributes," in *China's Ascent: Power, Security, and the Future of International Politics*, eds. Robert S. Ross and Zhu Feng (Ithaca, NY: Cornell University Press, 2008), 56.

[17] Zhu Feng, "China's Rise Will Be Peaceful: How Unipolarity Matters," in Ross and Zhu, 54.

[18] Ibid., 46.

biggest threat, but, regardless, has come to terms with its power in the current system, how does it grow power to move beyond the limits imposed on it? Its economy provides the answer, and sustained economic growth undergirds three imperatives.

First, since China began opening up in 1978, regime legitimacy has been derived more from economic growth and nationalist sentiment than from Communist ideological dogma—in the absence of political choice, contenting the masses was viewed as crucial for stability and therefore national survival. Yet fractures in the growth model began to manifest after nearly two decades of seemingly miraculous growth: China's status as the world's manufacturer of low-cost goods could only last so long, particularly given competition from other developing countries, resource scarcity, and environmental degradation.

Second, the 1990s highlighted Chinese vulnerability to potential US hard power coercion. The Gulf War, 1996 Taiwan Strait crisis, bombing of the Chinese embassy in Belgrade—all within the context of sanctions imposed on China after the Tiananmen massacre—demonstrated to China's leaders not only the technological overmatch of the US military but also America's potential to use it. Modernization to offset US strengths therefore depended upon resources provided by a growing economy.

Third, recasting the international order to a multipolar world not dominated by a hegemon relies upon diffusion of influence away from the United States. China's accession to the World Trade Organization in 2001 began its integration into a rules-based global economy. Today, however, China is less being integrated and more doing the integrating. The Asian Infrastructure Investment Bank, the One Belt/One Road development initiatives, its tentacular economic reach across Africa and South America—all highlight how far China has come in spreading its influence to forge multipolarity. "The most notable consequence of China's

economic rise for the pattern of the international politics will be the resulting increase not in China's coercive power (though this may occur), but in its political influence."[19]

How to realize those objectives, then, especially when confronted with an anarchic international system with a wildly asymmetric distribution of power, depends upon an effective strategy. China's strategic culture is suggestive. In Kissinger's survey of China, he argues that different cultural and historical experiences framed divergent conceptions of strategy between China and the West. "Where the Western tradition prized the decisive clash of forces emphasizing feats of heroism, the Chinese ideal stressed subtlety, indirection, and the patient accumulation of relative advantage."[20]

China analyst Timothy Thomas suggests that the Chinese approach to military strategy extends beyond ends, ways, and means considerations.[21] While focused on the PLA, Thomas' assessment offers salient points that underline a broader Chinese perspective on how it can favorably shape its external environment. Cultural, philosophical, and historical factors distinguish between the doctrinaire version of strategy as applied by the United States and a more ambiguous variant followed by China. Objective reality, manipulation, stratagems, *shi*—concepts generally unfamiliar to the US military (beyond occasional readings of the *Art of War*) yet figure highly in Chinese military literature.[22] Stratagems—"thought processes designed to mislead enemy perceptions, thinking, emotion, and will, to manipulate an adversary to one's advantage"[23]—could easily be applied at the nation-state (or corporate) level as they are at the

[19] Jonathan Kirshner, "The Consequences of China's Economic Rise for Sino-US Relations: Rivalry, Political Conflict, and (Not) War," in Ross and Zhu, 240.

[20] Henry Kissinger, *On China* (New York: Penguin Press, 2011), 23.

[21] Timothy Thomas, "China's Concept of Military Strategy," *Parameters* 44, no. 4 (Winter 2014-15): 39.

[22] Ibid., 40.

[23] Ibid., 42.

operational and tactical levels of war. Regardless of the application, the intent "is to 'induce' the enemy to make decisions the Chinese want."[24] Similarly, the concept of *shi* focuses on gaining "an advantage over an opponent after evaluating a situation and influencing it."[25] The highest form of *shi*, enabled by the use of stratagems, manifests itself when an opponent believes it is acting in its own interests yet is unwittingly serving another's.[26]

If obscuring intentions and biding time until favorable conditions emerge are fundamental aspects of China's strategic approach, and if China's national ascension depends upon the imperative of its economy, then manipulating and taking advantage of the United States is likely a purposeful policy.

"Peaceful Rise"

According to historian and Asian studies professor Robert Sutter, the "peaceful rise" concept matured as policy in 2003 and offered a "vision of China's future development that would be compatible with China's interests and those of its neighbors and concerned powers, notably the United States."[27] It recognized that, as a result of modernization since 1978, China's arrival on the world scene was amazing but incomplete: continued development and integration into the world economy was necessary to overcome the "contradictions" (i.e., individual and regional wealth disparity, resource scarcity, and environmental degradation) of its rise.[28] A peaceful world order was therefore a critical requirement; avoiding conflict with the United States, in particular, was fundamental.

---

[24] Thomas, "China's Concept of Military Strategy," 43.

[25] Ibid.

[26] Ibid., 44, 45.

[27] Robert G. Sutter, *China's Rise in Asia: Promises and Perils* (Lanham, MD: Rowman & Littlefield Publishers, 2005), 266.

[28] Ibid.

The key architect of "peaceful rise" was Zheng Bijian, a prominent and influential Chinese intellectual with broad experience in Chinese government and academia. Besides providing much of the intellectual basis that has served as China's narrative, he has also been its evangelist to the United States.[29] That Zheng also served, from 1992-1997, as the deputy of the Chinese Communist Party (CCP) Publicity Department (i.e., Ministry of Propaganda) is telling.[30]

In a 2005 speech at the Brookings Institution, Zheng reinforced the purpose of "peaceful rise" amid what he perceived as growing US criticism to its implications. China's perspective, he contended, based on the enormity of its size and the challenges it faced, was the long-view: to "realize basic modernization by the mid-twenty-first century…and catch up with medium-level developed countries."[31] Such development necessarily depended upon China embracing globalization and the international order that fostered it, yet in a singular way. Rather than "old-style industrialization" (beset with resource exploitation and environmental degradation), Great Power politics (manifested by the violence of pre-World War II Germany's and Japan's ascent and the shaking of the international order), and domestic tyranny, China's path would "transcend" such 20th century vestiges.[32] Dismissing notions of "hard power," such as military dominance or hegemony,[33] China instead would seek to gently reform the international system[34] and contribute to a multi-polar, globalized world. "China's peaceful rise is the ascent of a staunch force

[29] Zheng has written several articles, including for *Foreign Affairs*, and spoken at US think tanks.

[30] See "Zheng Bijian Biography," China Vitae, accessed January 4, 2016, http://www.chinavitae.com/biography/Zheng_Bijian/full.

[31] Zheng Bijian, *China's Peaceful Rise* (Washington, DC: Brookings Institution Press, 2006), 2.

[32] Ibid., 4.

[33] Ibid., 6-7.

[34] Ibid., 9.

defending rather than disrupting global peace. It is by no means a peril. It is a blessing for the world."[35]

Thematically, the "peaceful rise" narrative relied upon the logic of an inward-looking China to assuage external (read United States) concerns. China faced three "paradoxes" of its emergence: resource scarcity, environmental harm, and economic disparity.[36] Given the scope of the challenges and a mid-century goal of medium-level modernization, China would be too focused on its massive self-help project to pose a threat to regional neighbors or the international order.[37]

Certainly, Zheng was attempting to appeal to the values-based sentiment of a broader US audience to demonstrate that China's intentions were benign. By highlighting opportunities, common interests, and shared experiences, he sought to soften the impact of China's emergence in the minds of those most concerned about it. Yet "peaceful rise" was offered with caveats. According to Sutter, "the new approach remained contingent, and depended to a considerable degree on the United States continuing an overall cooperative approach toward China and its interests in Asian and world affairs."[38] Zheng's speech implied as much, with a call to action designed to spur on not both nations but primarily the United States.[39]

---

[35] Zheng, *China's Peaceful Rise*, 4.

[36] Ibid., 3.

[37] Ibid., 9.

[38] Sutter, *China's Rise*, 87-88.

[39] For example: Virtuous voices in America show that the United States is "beginning to face up to the reality of a peacefully rising China"; China's inability to overcome its challenges means that "not only will your worries remain, but China's peaceful rise will also be extremely difficult"; "If the United States can handle such trade disputes in an 'apolitical' way," then progress can be made; if only the United States could look at the forest through the trees, not focus on irritating details or possess "cold war thinking"; "It takes two hands to make a clap." Zheng, *China's Peaceful Rise*, 3, 10, 11, 13.

According to Robert Art, "the strategy of peaceful rise is the policy of a weak state, of a great power not yet arrived, but of one whose power is growing, that needs a peaceful environment for its power to continue to grow, and that wishes to avoid encirclement as it grows more powerful."[40]

Perhaps "peaceful rise," as Zheng contended, demonstrated an appealing and non-threatening Chinese vision of the future that complemented the existing international order. But given China's recent assertiveness enabled by the methodical growth of its considerable economic, political, and military clout, perhaps "peaceful rise" was instead a stratagem designed to create *shi*—a means to manipulate the United States until China had the strength to confront the world on its own terms.

Five Year Plans

If "peaceful rise" has been its narrative, how has China—with its long view—realized its economic ambitions? China's Five Year Plans, particularly in the rising China era, are expressions of national strategy and serve as "Beijing's core mechanism for coordinating and implementing policy across national ministries and local governments."[41] The role the plans play underscore the subsequent behavior of state institutions both domestically and internationally and set conditions for the environment in which they operate.

Mao implemented the Five Year Plans, modeled on the Soviet system, to reestablish China as a global power following the "century of humiliation." Given the absence of competitive

[40] Robert J. Art, "The United States and the Rise of China: Implications for the Long Haul," in Ross and Zhu, 262.

[41] Oliver Melton, "China's Five-Year Planning System: Implications for the Reform Agenda," in *China Ahead of the 13th Five-Year Plan: Competitiveness and Market Reform: Hearing before the US-China Economic and Security Review Commission,* 114th Cong., 1st sess., April 22, 2015, 42, accessed December 01, 2015, http://origin.www.uscc.gov/sites/default/files/transcripts/April%2022%2C%202015%20Hearing%20Transcript.pdf.

free markets and the ideological need to adhere to a socialist system, Five Year Plans coupled "'top-down' commandism with 'bottom up' mobilisation to develop production and for social advance."[42] As a condition of the Cold War and the struggle between the two superpowers, which necessarily limited China's ability to reach outwards, the plans under Mao's leadership sought to create a state with a degree of self-sufficiency and self-reliance.[43]

After Mao, however, the plans changed in scope and intent. Given the transition away from an insular, inward-looking nation toward a regional and global powerhouse with an expansive worldview, the plans have focused less on strict production quotas to shape economic output and more on "guides to how leaders want to steer the country."[44] Instead of edicts that specify how many bushels of grain or tons of steel or number of tractors that state-owned enterprises should produce, the plans now represent national strategies around which the state's institutions—all levels of government, state enterprises, and presumably private companies—coalesce.[45] Five Year Plans represent the priorities—and therefore illuminate likely motivations—of the CCP.

In current form, China's approach to national strategy development and execution is "whole of government." Five Year Plans are not simply top-down impositions by Party leadership on subordinate institutions and society in a set timeframe. Instead, Five Year Plans are sufficiently broad guideposts that enable development of more detailed implementation plans at subordinate levels in a multi-year process—"a dynamic institution for systematically bringing information up from the grassroots to the central government, processing and analyzing that

---

[42] Jenny Clegg, *China's Global Strategy Towards a Multipolar World* (New York: Pluto Press, 2009), 125.

[43] Ibid.

[44] S.R., "The Economist Explains: Why China's Five-Year Plans are So Important," *The Economist Explains* (blog), *Economist*, October 26, 2015, accessed December 01, 2015, http://www.economist.com/blogs/economist-explains/2015/10/economist-explains-24.

[45] Ibid.

information to support policy decision, delegating and coordinating the implementation process across the bureaucracy, and then monitoring the effectiveness of those policies."[46] Such an approach is necessarily inclusive and sticky: it cements lower level plans with overarching national goals, involves all layers of the bureaucracy but also participation from non-governmental third-parties, and, through such "buy in," enhances and preserves the legitimacy of the government.[47] This is not to say that decisionmaking and policy execution are monolithic; there are certainly challenges associated with layers of the bureaucracy, competing organizational and individual interests, and incentivization of bad behavior (i.e., corruption, poor investment decisions, cooking the books).[48] Yet the point is that the state—its institutions and society as a whole—is generally oriented to accomplish big things if it chooses.

As the 21st century began, China's 10th Five Year Plan (covering 2001-2005) continued to focus on the rapid growth that had established China as the world's manufacturing center. While that plan acknowledged significant (but not overriding) issues relating to factors other than economic growth (such as the environment, rural development, and healthcare), it wasn't until the 11th Five Year Plan (covering 2006-2010) that Party leadership began shifting in a new direction.

The major themes of the 11th Five Year Plan—"scientific concept of development" and "building a harmonious society"—highlighted four significant transitions based on the relationship between the nature of the Chinese economy, people, and the environment. First, the plan called for economic development based not, primarily, on investment and export but instead on domestic consumption in order to ensure a more stable economy—to shift from "quantitative to qualitative growth."[49] The economic model based on cheap production could only last so long

[46] Melton, "China's Five-Year Planning System," 43.

[47] Ibid., 45-47, 51-52.

[48] Ibid., 47-49, 54.

[49] Letian Pan, ed., "Ten Features in China's 11th Five Year Plan," *People's Daily*, March 8, 2006, accessed December 20, 2015, http://www.gov.cn/english/2006-

given that it resulted in a diminished competitive edge as resources became more expensive and impacted profit margins with the added costs of preserving the environment.[50] Second, the plan claimed "a national strategy" to become an innovation engine and regarded "the enhancement of independent innovation capabilities as the central link" to a new future.[51] Science and technology, education, and more say in foreign investment (including use of "advanced foreign technologies") would be crucial to indigenous innovation.[52] Third, the plan targeted improvements to environmental protection. Whereas ravenous consumption of raw materials had been vital for China's explosive growth, such a resource-intensive model was unsustainable.[53] Increasing resource scarcity at home and abroad made production more expensive; pillaging of natural resources coupled with ecologically unfriendly industrial production soured the environment and created social discontent. Finally, the plan highlighted reforms "with the most direct and practical issues that concern the interests of the masses."[54] With policy targets that focused on social issues (such as urban employment, rural development, healthcare, and public services), the plan acknowledged the importance of translating the benefits of China's economic miracle into improving the lives of its citizens. Undoubtedly, preserving stability was at the forefront of leadership calculations.

The 12th Five Year Plan (covering 2011-2015) reinforced the strategic objectives of the previous plan and focused on transitioning the economy from a high-growth export-based model

---

03/08/content_246945.htm.

[50] Ma Kai, "The 11th Five-Year Plan: Targets, Paths, and Policy Orientation," National Development and Reform Commission, March 19, 2006, accessed December 27, 2015, http://www.gov.cn/english/2006-03/23/content_234832.htm.

[51] Ibid.

[52] Letian Pan, ed., "Ten Features," and Letian Pan, ed., "Abstract of the Eleventh Five-Year Plan outline (draft)," *People's Daily*, March 8, 2006, accessed December 20, 2015, http://www.gov.cn/english/2006-03/08/content_246973.htm.

[53] Ma Kai, "The 11th Five-Year Plan."

[54] Letian Pan, ed., "Abstract of the Eleventh."

to a high-quality domestic-consumption one.[55] "This is seen as necessary to ensure greater social stability by increasing the benefits that accrue to the average household from China's strong GDP growth."[56] Yet the plan also reflected "a continuation of a long term strategy of capability building,"[57] derived primarily from innovation. "Policymakers at the national and local level seem almost exclusively focused on improving China's ability to develop advanced technologies and capture larger and more sophisticated segments of global manufacturing networks."[58] To help foster domestically inspired innovation, the plan specified seven Strategic Emerging Industries (which would be privileged with resources and largely protected from foreign competition) central to transforming the economy from one based on industrial manufacturing to one based on indigenous creativity.[59] A focus on "products with high intellectual content, and not just products with high labor content"[60] suggested a desire to compete with, and potentially dominate, US and European companies on the global market.

While the 13th Five Year Plan (covering 2016-2020) won't be released until late Spring 2016, the Fifth Plenary Session of the Central Committee adopted what are regarded as its broad objectives. In addition to abolishing the "one child" policy, the next plan will likely focus on improving society (including doubling GDP per capita, eliminating rural poverty, expanding

---

[55] Nicholas Consonery, "Testimony before the US-China Economic and Security Review Commission," in US-China Economic and Security Review Commission, April 22, 2015, 31.

[56] Eswar S. Prasad, "The Path to Sustainable Growth in China," in US-China Economic and Security Review Commission, April 22, 2015, 162.

[57] Willy C. Shih, "Prepared Statement of Dr. Willy C. Shih," in *China's Five-Year Plan, Indigenous Innovation and Technology Transfers and Outsourcing: Hearing before the US-China Economic and Security Review Commission*, 112th Cong., 1st sess., June 15, 2011, 29, accessed December 3, 2015, http://origin.www.uscc.gov/sites/default/files/transcripts/6.15.11HearingTranscript.pdf.

[58] Melton, "China's Five-Year Planning System," 53.

[59] Shih, "Prepared Statement," 28-29, 33. The industries included energy saving and environmental protection, IT, bio industries, high-end assembly and manufacturing, new energy sources, new materials, and new energy powered cars.

[60] Ibid., 29.

health care and housing, and protecting the environment), maintaining and expanding reforms that shift economic growth to a consumption model (as well as consolidating and improving the efficiency of state-owned enterprises), and reinforcing domestic innovation (including "mass entrepreneurship" and a tighter integration between the Internet and the economy).[61]

Importantly, China will "upgrade the economy into a global manufacturing power [and] cultivate strategic industries" while simultaneously implement a national "negative list" that puts key areas "off limits to foreign investment."[62] According to Nicholas Consonery, the Chinese government will "tighten state control over strategic sectors of the economy, particularly those earmarked for greater international expansion or identified as strategic for national security reasons."[63] To that end, it will drive the development of national champions—"globally competitive national brands in strategic industries"[64]—to compete with the Boeings, GEs, and Fords of the world. Furthermore, "the government's willingness to invest significantly in new and emerging technologies will indeed mean greater competitive capabilities for Chinese firms in a range of high-tech sectors. It will also mean continued regulatory preferences for [state-owned enterprises] in key sectors in ways that sustain advantages for those firms vis-à-vis US or other foreign firms in the China market."[65]

Five Year Plans, as expressions of state decision- and policy-making, are emerging strategies.[66] Such an incremental approach affords opportunities to react, respond, and reshape

---

[61] Andrew Moody, "Dissecting China's Five-Year Plan," *The Telegraph*, November 23, 2015, accessed December 15, 2015, http://www.telegraph.co.uk/sponsored/china-watch/politics/12006280/china-five-year-plan.html; Xinhua News Agency, "Xinhua Insight: China's New Five-Year Plan Covers Home Stretch to Prosperity," Xinhuanet, October 30, 2015, accessed December 15, 2015, http://news.xinhuanet.com/english/2015-10/30/c_134764096.htm.

[62] Xinhua News Agency, "Xinhua Insight."

[63] Consonery, "Testimony," 36.

[64] Ibid., 37.

[65] Ibid., 37.

[66] They also depend upon nested, subordinate plans for additional detail. Two important

objectives. In discussing how plans and implementation are formed over years, Oliver Melton says the process "creates space for China's distinctive method of policy experimentation and pilot projects, which often precede national plans and are used to inform subsequent implementation details."[67] Periodic reviews and assessments feed back into the system—"spreading successful models and correcting unsuccessful ones"[68]—that in turn shape the development of subsequent Five Year Plans: the 11th began to change the direction of the country, the 12th took it to the next level[69], and the 13th will likely reinforce those priorities.[70] Which gets to the point: China has proven its ability to follow a purposeful, consistent way ahead based on its perception of national interests and objectives. Past is prologue.

China has institutionalized the requirement to innovate. Indeed, China fundamentally *depends* upon innovation to secure its future. Yet innovation must incubate and grow in necessary conditions (resource commitments, research, education, culture), which expose a paradox given the challenges it must overcome—the contradictions of its rise. The government's dilemma is compounded most by what it believes it possesses least: namely, time. Despite its self-regard as

examples: In 2006, China released the *Medium- and Long-Term National Plan for Science and Technology*, the first formal articulation of the imperative of "indigenous innovation" to supplant Western technology (especially IT) with homegrown variants. China began to modify the playing field domestically (by encouraging local development) and internationally (by limiting market access to foreign companies, compelling them to share proprietary and trade secret information, or shutting them out completely). See John Neuffer, "Testimony before the US-China Economic and Security Review Commission," in US-China Economic and Security Review Commission, June 15, 2011, 81-86. In May 2015, China unveiled "Made in China 2025" that outlines ten economic sectors in which China must compete, innovate, and win in order to preserve its dominance in manufacturing while simultaneously moving up the value chain. "Made in China 2025" targets areas long-dominated by the United States, from IT to medical products to robotics to commercial airplanes to clean energy vehicles to agricultural equipment. See Scott Kennedy, "Made in China 2025" (Washington, DC: Center for Strategic and International Studies, June 1, 2015), accessed December 1, 2015, http://csis.org/publication/made-china-2025.

[67] Melton, "China's Five-Year Planning System," 44.

[68] Ibid., 45.

[69] Ibid., 52.

[70] Ibid., 49.

the nation of history, despite its penchant for and success at long-term planning, despite the decades long implications of "peaceful rise," it believes the first half of the 21st century—and in particular the first twenty years—represent its window of opportunity.[71] According to Xi's vision, by 2021 China will be a "moderately prosperous society." By 2049, the "China Dream" will be fulfilled.[72] Time, to the extent that there is enough of it to transform a headwind economy before it fails to meet the expectations of a dreaming population, becomes its own imperative.

If the future of the economy depends upon a transition to a high-technology, consumption-based model built on national champions that can dominate domestic and international markets, and if a sustainable economy is vital for the preservation of the Party, cultivation of a state-of-the-art military, and expansion of China's global influence, then the notion of a fleeting window of opportunity leads to an important conclusion. "It is much more efficient for the Chinese to steal innovations and intellectual property—the 'source code' of advanced economies—than it is for them to incur the cost and time of creating their own."[73]

And what better way to catch up or leap ahead than by exploiting the most technologically advanced country—especially if it refuses to push back?

US Response to Cyber Economic Espionage

China's rise has been met with significant policy and strategy debate on how the United States should respond to it.[74] Whether relating to the "Asia-Pacific Rebalance" or the Trans-Pacific Partnership or reinvigorated relationships with allies, the United States has expended diplomatic, economic, and military energy as China has become more regionally assertive. Yet to

[71] Kissinger, *On China*, 497-498.

[72] Xinhua News Agency, "Xi pledges."

[73] McConnell, Chertoff, and Lynn.

[74] See, for example, Michael Lumbers, "Whither the Pivot: Alternative US Strategies for Responding to China's Rise," *Comparative Strategy* 34, no. 4 (September-October 2015): 311-329, accessed January 27, 2016, http://dx/doi.org/10.1080/01495933.2015.1069510.

the extent that China's ascent has been potentially enabled by the cyber theft of US intellectual property, the United States has only incrementally attempted to address the problem.

Publicly acknowledged awareness of the issue and its presumed threat to national security became apparent late in President Obama's first administration—but limited policy success, particularly as measured by passed legislation, was only achieved towards the end of his second term. Understanding the reasons for such a delayed response is partially illuminated by the history of the administration's actions within the context of domestic politics, the influence of the private sector, and the effectiveness of government narratives to garner support while simultaneously signaling potential consequences to dissuade China.

Chronology

Just as cyberspace has evolved, so too has the government's response on how to secure it. Cyberspace's technological complexity (routers, switches, servers, computers, protocols, all connected in a dizzying mesh of billions of nodes) is matched by its social complexity—a dynamic relationship between social behavior (for instance, how we learn, communicate, interact, and conduct economic transactions) and culture, laws, rights, policies, and authorities. Such complexity and novelty makes it difficult for policymakers to arrive at enduring conclusions.

Yet while the administration has been on more of a simmer, it has remained remarkably consistent in its goals: legislation aimed at improving information sharing between the public and private sector, establishing international norms of acceptable behavior in cyberspace, and increasing public awareness. While none of the efforts are specifically aimed at China, they are, by extension and in large part, because of China and suspicions that it was siphoning American intellectual property through exploitation of cyberspace.

2009

Shortly after taking office, the president initiated a 60-day cyberspace policy review. Released on May 29, key elements of the review would endure through 2015. At a press conference, the president said, "America's economic prosperity in the 21st century will depend on cybersecurity." Highlighting an overall level of unpreparedness, lack of investment, and policy incoherence, the president's plan sought to shape a better future. "So a new world awaits—a world of greater security and greater potential prosperity—if we reach for it, if we lead."[75]

The plan acknowledged the importance of cybersecurity, the cost of cybercrime and intellectual property theft, and the need for a "national dialogue" to improve awareness of shared threats while protecting privacy and civil liberties—yet it failed to articulate specific timelines or specific threats. What it did, specifically, address was the fact that things must change: "The United States must signal to the world that it is serious about addressing this challenge." [76]

The plan, above all, demonstrated that the government couldn't do it alone but would instead need to cultivate the private sector, Congress, the American people, and the international community in order to improve security and diminish the threats.[77] Information sharing and coordinated actions, particularly between businesses and with the government, would be key[78]—but would also be complicated by the tension between the public and private sectors as well as by the nature of cyberspace. The government would need to balance its responsibility to protect the nation and preserve security, without meddling too much, at the same time as the terrain most

[75] White House, *Securing Our Nation's Cyber Infrastructure.*

[76] White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (n.d. but released on May 29, 2009), i,iii, accessed October 28, 2015, https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[77] Ibid., iv.

[78] Ibid., 17

threatened would be owned by businesses.[79] The plan acknowledged that legal and regulatory impediments inhibited the sharing of information, including antitrust and trade laws, corporate liability and reputational concerns, exposure of proprietary information, privacy rights and civil liberties, and classified information restrictions.[80]

The plan identified ten near-term and 14 mid-term actions. To ensure forward movement and unity of effort amidst a vexing array of technological, legal, and political challenges with layers of stakeholders, the administration would need a cybersecurity official to coordinate actions and "anchor [l]eadership at the White House."[81]

Nonetheless, the president would not appoint his Cybersecurity Coordinator until seven months later.[82]

2010

As 2010 began, alleged Chinese cyber malfeasance hit one of the key US "national champions" in the Information Age economy. Google, after prolonged tensions with the Chinese government relating to censorship, reported that it had been the victim of a sophisticated cyber attack designed to steal proprietary information and spy on Chinese dissidents. The attack targeted at least 20 other companies, although that number would eventually grow to 34.[83] The

[79] White House, *Cyberspace Policy Review*, iv.

[80] Ibid., 18-19.

[81] Ibid., 7.

[82] Ellen Nakashima, "Obama to Name Howard Schmidt as Cybersecurity Coordinator," *Washington Post*, December 22, 2009, accessed January 14, 2016, http://www.washingtonpost.com/wp-dyn/content/article/2009/12/21/AR2009122103055.html. See also Ellen Nakashima, "Cybersecurity Official Resigns Over Delays in Appointment," *Washington Post*, August 4, 2009, accessed January 14, 2016, http://www.washingtonpost.com/wp-dyn/content/article/2009/08/03/AR2009080302697.html. The delay, apparently, led to the resignation of the official responsible for producing the cyberspace policy review.

[83] David Drummond, "A New Approach to China," Google Official Blog, January 12, 2010, accessed January 15, 2016, https://googleblog.blogspot.com/2010/01/new-approach-to-china.html; Dancho Danchev, "Google-China Cyber Espionage Saga: FAQ," ZDNet, January 19, 2010, accessed January 15, 2016, http://www.zdnet.com/article/google-china-cyber-espionage-

announcement would eventually lead to Google pulling out of the Chinese market. The administration publicly responded through Secretary of State Clinton, who said, toward the end of a speech on Internet freedom, that China should "conduct a thorough investigation."[84]

Despite other attacks and cybersecurity incidents (including a 20 minute rerouting of a "large volume" of US Internet traffic, especially many US government domains and commercial websites, through Chinese servers owned by China Telecom[85], the July appearance of Wikileaks, and the October discovery of Stuxnet[86]), few accomplishments were evident save for the president proclaiming October as "National Cybersecurity Awareness Month" and the unveiling of a Department of Homeland Security (DHS) and Federal Trade Commission online cybersecurity awareness campaign.

2011

Cybersecurity filled headlines. In March, RSA announced that its SecurID system had been compromised, with cascading effects in the defense industry[87] (including Lockheed Martin, which reported a "significant and tenacious attack" in May.)[88] In April, the Sony Playstation Network was hacked, exposing 77 million user accounts.[89] In May, Google reported alleged

saga-faq/.

[84] Hillary Rodham Clinton, "Remarks on Internet Freedom" (speech, Newseum, Washington, DC, January 21, 2010), accessed January 15, 2016, http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

[85] US-China Economic and Security Review Commission, *2010 Annual Report to Congress of the US-China Economic and Security Review Commission*, 111th Cong., 2d sess., (Washington, DC: US Government Printing Office, November 2010), 241, 244.

[86] Center for Strategic and International Studies, "Significant Cyber Incidents Since 2006" (Washington, DC: Center for Strategic and International Studies), item 70, accessed November 30, 2015, http://csis.org/files/publication/160406_Significant_Cyber_Events_List.pdf.

[87] Ibid., item 81.

[88] Lockheed Martin, "Lockheed Martin Customer, Program and Employee Data Secure," press release, May 28, 2011, accessed January 14, 2016, http://www.lockheedmartin.com/us/news/press-releases/2011/may/LockheedMartinCustomerPro.html.

[89] Will Ripley, "Why Sony Hasn't Learned Lessons of 2011 Playstation Hack," CNN,

Chinese attempts to steal passwords of Gmail users, including those of US officials and Chinese activists.[90] In August, McAfee released a report detailing Operation Shady RAT, an advanced persistent threat that had stolen intellectual property going back to at least 2006 from 49 US companies[91]; while McAfee didn't definitively attribute China, the report inferred as much.[92] In October, Symantec reported 27 US companies involved in chemicals and advanced materials development were targeted for intellectual property theft by hackers in China.[93] In December, the *Wall Street Journal* reported that Chinese hackers had penetrated US Chamber of Commerce networks since at least 2009.[94]

The administration, almost two years after it completed its cyberspace policy review, began to take action. In May (after Sony's announcement but before Google's), it released three documents.

The first was its *International Strategy for Cyberspace*. Aspirational (and reminiscent of Secretary Clinton's speech nearly 18 months earlier), the strategy highlighted the administration's

---

December 18, 2014, accessed January 14, 2016, http://www.cnn.com/2014/12/18/ world/ asia/sony-hack-lab-ripley/.

[90] Cecilia Kang, "Google: Hundreds of Gmail Accounts Hacked, Including Some Senior US Government Officials," *Washington Post*, June 1, 2011, accessed January 14, 2016, https://www.washingtonpost.com/blogs/post-tech/post/google-hundreds-of-gmail-accounts-hacked-including-some-senior-us-government-officials/2011/06/01/AGgASgGH_blog.html.

[91] Dmitri Alperovitch, *Revealed: Operations Shady RAT: White Paper Version 1.1* (Santa Clara, CA: McAfee, 2011), accessed January 13, 2016, http://www.mcafee.com/us/resources/ white- papers/wp-operation-shady-rat.pdf. RAT is an acronym for "remote access tool."

[92] Michael Joseph Gross, "Exclusive: Operation Shady Rat—Unprecedented Cyber-espionage Campaign and Intellectual-Property Bonanza," *Vanity Fair*, August 31, 2011, accessed January 13, 2016, http://www.vanityfair.com/news/2011/09/operation-shady-rat-201109.

[93] Center for Strategic and International Studies, "Significant Cyber Incidents Since 2006," item 96; Eric Chien and Gavin O'Gorman, *The Nitro Attacks: Stealing Secrets from the Chemical Industry* (Mountain View, CA: Symantec, 2011), 1,3, accessed January 14, 2016, http://www.symantec.com/content/en/us/ enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf.

[94] Siobhan Gorman, "China Hackers Hit US Chamber," *Wall Street Journal*, December 21, 2011, accessed January 14, 2016, http://www.wsj.com/articles/ SB10001424052970204058404577110541568535300.

desire to promote a global Internet that adhered to "core commitments"—preservation of fundamental freedoms, privacy, and the free flow of information.[95] The United States would, working through bilateral and multilateral venues, seek to develop norms of behavior and international standards (including intellectual property protection and cybercrime policy), strengthen partnerships, build military capabilities and expand cooperation with allies and partners, and promote a broader concept of Internet governance that would not see the United States as the single rule-maker. The second document was its legislative proposal to Congress, the administration's first related to cybersecurity. The proposal reflected the major conclusions of the 2009 cyberspace policy review, and included legislative requests to standardize data breach reporting (consolidating 47 state laws into one federal statute) to inform consumers of the exposure of their personal or financial information; streamline government ability to assist at the corporate, state, or local level (but relating only to critical infrastructure protection); permit voluntary cyber threat and incident information sharing with government and industry, with certain legal immunity provisions; update laws to improve law enforcement ability to investigate and prosecute computer crimes; and establish a framework for protecting individual privacy.[96] The final document released was not policy at all but instead a list of accomplishments that showed completion of the near-term objectives of the 2009 policy review.[97]

---

[95] Barack Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, May 2011), 5, accessed January 13, 2016, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[96] White House, Office of the Press Secretary, *Fact Sheet: Cybersecurity Legislative Proposal*, May 12, 2011, accessed January 13, 2016, https://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal.

[97] White House, Office of the Press Secretary, *Fact Sheet: The Administration's Cybersecurity Accomplishments*, May 12, 2011, accessed January 13, 2016, https://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-administrations-cybersecurity-accomplishments. The document highlighted improvements to how the federal government protects its own networks, development of a public-private response plan for significant cyber events that threaten critical infrastructure, and the roll-out of a public awareness

While certainly the administration had been formulating plans and developing federal institutional infrastructure (for instance, clarifying the roles and responsibilities of the Department of Homeland Security or establishing US Cyber Command), the fact remains that two years had passed with few policy overtures. As it was, no legislation was passed.

In October, the Office of the National Counterintelligence Executive released a report, *Foreign Spies Stealing US Economic Secrets in Cyberspace*, that detailed "significant and growing threats to the nation's prosperity and security."[98] Importantly, the report's release seemed to suggest that America's patience was wearing thin. "It marked the first time that the US government had publicly and unequivocally named China as a source of some of the most aggressive cyberspying. Until then, US officials had largely confined their complaints to off-the-record remarks to journalists, calibrated not to disrupt diplomatic relations with one of the country's most important trading partners."[99]

Despite the rash of publicly reported cyber incidents (related to China or otherwise)—and perhaps because of the lack of national consensus (at least with Congress) and armed with its new international strategy—the administration focused on diplomacy in dealing with China.[100]

2012

Cyber incidents in 2012 continued to highlight the vulnerabilities of connecting to the Internet. In February, NASA reported a widespread hack of the Jet Propulsion Laboratory, linked to computers in China.[101] In March, DHS reported on-going attempts to exploit the industrial

---

campaign.

[98] Office of the National Counterintelligence Executive, i.

[99] Shane Harris, "Exclusive: Inside the FBI's Fight Against Chinese Cyber-Espionage," *Foreign Policy*, May 27, 2014, accessed November 2015, http://foreignpolicy.com/2014/05/27/exclusive-inside-the-fbis-fight-against-chinese-cyber-espionage/.

[100] Michael Joseph Gross, "Enter the Cyber-dragon," *Vanity Fair*, August 31, 2011, accessed January 13, 2016, http://www.vanityfair.com/news/2011/09/chinese-hacking-201109.

[101] US Government Accountability Office, *Cybersecurity: National Strategy, Roles, and*

control systems of gas pipelines.[102] On August 15, an attack against Saudi Aramco destroyed nearly 35,000 workstations and threatened to impact the global supply of oil.[103] In September, several large American banks suffered denial of service attacks.[104]

As an election year, the first half of 2012 seemed to point to an administration more willing to go public. During his State of the Union address on January 24, the president mentioned, for the first time, the need for improved cybersecurity and the legislative proposal he had sent to Congress the previous year (although there was no acknowledged connection with China).[105] Three days later, the McConnell, Chertoff, and Lynn editorial connecting China to cyber economic espionage appeared in the *Wall Street Journal*.

As the window for legislation began to close with the pending November elections, the president wrote an op-ed piece in the July 20 *Wall Street Journal* and called for the Senate to pass the 2012 Cybersecurity Act. (Alexander's "greatest transfer of wealth in history" speech preceded the article by just over a week.) Yet in August, despite bipartisan recognition of the significance of cybersecurity, political polarization prevented a workable compromise; Senate Republicans filibustered the bill given that it "would be too burdensome for corporations."[106]

Responsibilities Need to Be Better Defined and More Effectively Implemented (GAO-13-187), February 2013, 10, accessed January 14, 2016, http://www.gao.gov/assets/660/652170.pdf.

[102] Center for Strategic and International Studies, "Significant Cyber Incidents Since 2006," item 104.

[103] Jose Pagliery, "The Inside Story of the Biggest Hack in History," CNNMoney, August 5, 2015, accessed January 14, 2016, http://money.cnn.com/2015/08/05/technology/aramco-hack/.

[104] Center for Strategic and International Studies, "Significant Cyber Incidents Since 2006," item 120.

[105] White House, Office of the Press Secretary, *Remarks by the President in State of the Union Address*, January 24, 2012, accessed January 19, 2016, https://www.whitehouse.gov/the-press-office/2012/01/24/remarks-president-state-union-address.

[106] Michael Schmidt, "Cybersecurity Bill is Blocked in Senate by G.O.P. Filibuster," *New York Times*, August 2, 2012, accessed January 13, 2016, http://www.nytimes.com/2012/08/03/us/politics/cybersecurity-bill-blocked-by-gop-filibuster.html.

Regardless of the administration's attempts at building a consistent narrative—the counterintelligence report detailing corporate espionage, well-timed commentary in prominent news outlets, official and unofficial statements—election year politics trumped consensus.

2013

In the absence of legislative support yet with continued reports of Chinese cyber economic espionage, the administration in 2013 began to take unilateral executive action as well as continued to build the case for the impact on the United States of intellectual property theft—and China's role as the chief culprit. The year would be more confrontational, but also revelatory.

The Defense Science Board released a report in January after an 18-month study of cyber threats. While it focused on the military aspects of information technology (IT), it also included an assessment of cyber-enabled economic espionage. "The long term loss of so much intellectual property and capability will result in a *serious competitive disadvantage* to the US economy."[107]

During his State of the Union address, the president highlighted cybersecurity (three paragraphs instead of the single, off-hand sentence in 2012) and the dangers posed to individual identity, critical infrastructure, and intellectual property. "We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."[108] He called on Congressional action but in the interim would rely on his executive powers to improve the nation's posture.

[107] Department of Defense, Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, January 2013), 31, accessed January 8, 2016, http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf. Emphasis in original.

[108] White House, Office of the Press Secretary, *Remarks by the President in the State of the Union Address*, February 12, 2013, accessed January 19, 2016, https://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address.

The next day, the president released Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." The order directed various elements of the Executive Branch (primarily under the lead of DHS) to improve information sharing with the private sector (particularly critical infrastructure owners and operators) and establish a voluntary framework for adoption of technology standards, information sharing, incident response, and best practices.[109]

The president's action followed reports that the *New York Times*, *Wall Street Journal*, *Washington Post*, and *Bloomberg News* had been hacked by Chinese actors.[110] A groundbreaking report by a private Internet security firm a week later, however, would steal the headlines.

On February 19, Internet security firm Mandiant released a detailed exposition on what it said was evidence of a long-running (since at least 2006) Chinese-government cyber economic espionage campaign that targeted 115 US "victims."[111] Mandiant was clear that what it called "Advanced Persistent Threat 1" was a PLA unit whose purpose was to "steal broad categories of intellectual property."[112] The report also noted that many of the targeted corporations were in four of the seven Strategic Emerging Industries linked to China's 12th Five Year Plan.[113]

The next day, the administration released the *Administration's Strategy on Mitigating the Theft of US Trade Secrets*. The strategy set five objectives, all thematically similar to the

---

[109] Barack Obama, Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," *Federal Register* 78, no. 33 (February 12, 2013); Department of Homeland Security, *Fact Sheet: EO 13636 Improving Critical Infrastructure Cybersecurity and PPD-21 Critical Infrastructure Security and Resilience*, March 2013, accessed January 13, 2016, https://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf.

[110] Nicole Perlroth, "Washington Post Joins List of News Media Hacked by the Chinese," *New York Times*, February 1, 2013, accessed January 19, 2016, http://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html.

[111] Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Alexandria, VA: Mandiant, 2013), 2, 21, accessed November 23 2015, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[112] Ibid., 3.

[113] Ibid., 4.

administration's cybersecurity objectives: use diplomacy and work through international frameworks to better protect trade secrets; encourage voluntary best practices for companies to safeguard intellectual property; improve law enforcement ability to investigate and prosecute economic espionage; update domestic laws; and raise public awareness.[114]

In March, the administration for the first time specifically highlighted China's role in cyber theft.[115] During a speech about the rebalance to the Pacific at the Asia Society New York, national security advisor Thomas Donilon said that the issue of cyber espionage was now coloring the relationship between the world's two largest economies: "I am not talking about ordinary cybercrime or hacking…Increasingly, US businesses are speaking out about their serious concerns about sophisticated, targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China on an unprecedented scale."[116] In May, the Department of Defense released its annual report to Congress on Chinese military developments, and specifically highlighted an apparent connection between the PLA and widespread "exfiltrating information" cyber incidents in 2012.[117] Later, at a speech in Singapore, Secretary of Defense Hagel gave "one of the most direct rebukes from the US" of Chinese cyber activity.[118] At the same time, the Commission on the Theft of American Intellectual Property released its report.

---

[114] Victoria Espinel, "Launch of the Administration's Strategy to Mitigate the Theft of US Trade Secrets," White House blog, February 20, 2013, accessed January 22, 2016, https://www.whitehouse.gov/blog/2013/02/20/launch-administration-s-strategy-mitigate-theft-us-trade-secrets.

[115] Harris, "Exclusive: Inside the FBI's Fight."

[116] Thomas Donilon, "The United States and the Asia-Pacific in 2013" (speech, Asia Society New York, March 11, 2013, accessed January 8, 2016, http://asiasociety.org/new-york/complete-transcript-thomas-donilon-asia-society-new-york.

[117] Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (Washington, DC: Office of the Secretary of Defense, 2013), 36, accessed January 14, 2016. http://www.defense.gov/Portals/1/Documents/pubs/2013_China_Report_FINAL.pdf.

[118] "Chuck Hagel Accuses China Over 'Cyber Intrusions'," BBC, June 01, 2013,

But building on the momentum of an executive order, scathing reports, and more pointed public statements would be short-lived as the administration dealt, in June and for months following, with the fallout from documents stolen and leaked by an NSA contractor. Less than a week after the *Guardian*'s initial release, during a summit with Xi Jinping in California, the president highlighted specific examples of Chinese intellectual property theft—the first direct discussion of the issue between both leaders[119]—yet no agreement between the two countries would occur for more than two years.

2014

Cyber incidents in 2014 would be singular for both the enormity of compromised accounts as well as growing public awareness of alleged nation-state hacking.

Millions of people had to contend with the potential of identity theft, particularly given the increasing scope and scale of corporate database breaches involving account information for a significant portion of the American population. Hackers compromised 110 million accounts at Target in January, 83 million at major banks in August, and 56 million at Home Depot in September.[120] Government networks (and government employees) were also targeted, including hacks of the State Department, the White House, the National Oceanic and Atmospheric Administration, the US Postal Service, OPM, and a contractor responsible for security clearance information.[121]

accessed January 19, 2016, http://www.bbc.com/news/world-us-canada-22739436.

[119] David E. Sanger, "Obama and Xi Try to Avoid a Cold War Mentality," *New York Times*, June 9, 2013, accessed January 10, 2016, http://www.nytimes.com/2013/06/10/world/asia/obama-and-xi-try-to-avoid-a-cold-war-mentality.html?_r=0.

[120] Sharone Tobias, "2014: The Year in Cyberattacks," *Newsweek*, December 31, 2014, accessed January 20, 2016, http://www.newsweek.com/2014-year-cyber-attacks-295876.

[121] Center for Strategic and International Studies, "Significant Cyber Incidents Since 2006," item 170, 171, 172, 158, 155.

For its part, the administration stayed the course, unveiled another element of its 2009 review, and continued to adhere to its basic message. On February 12, the administration announced the launch of the Cybersecurity Framework, a key component of the 2013 Executive Order 13636. Developed by the National Institute of Standards and Technology (NIST) in conjunction with the private sector, the voluntary framework "uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses."[122] While primarily designed for owners and operators of US critical infrastructure, the framework was designed for broader application, including "as a model for international cooperation"[123] and to help corporate leaders make informed risk decisions to improve cybersecurity.[124]

Yet events would also demonstrate that the administration had a newfound muscularity.

In May, the Justice Department released a 31-count indictment against five PLA officers—the first legal action taken by the United States in response to Chinese cyber economic espionage. The indictment accused the officers of conducting a cyber campaign designed to steal US corporate information to benefit Chinese state-owned enterprises.[125] China was incensed.[126]

---

[122] National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.0*, 1, February 12, 2014, accessed January 20, 2016, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[123] Ibid., 1-2.

[124] White House, Office of the Press Secretary, *Background Briefing on the Launch of the Cybersecurity Framework*, February 12, 2014, accessed January 20, 2016, https://www.whitehouse.gov/the-press-office/2014/02/12/background-briefing-launch-cybersecurity-framework.

[125] Department of Justice, Office of Public Affairs, *US Charges Five Chinese Military Hackers for Cyber Espionage Against US Corporations and a Labor Organization for Commercial Advantage*, May 19, 2014, accessed January 20, 2016. http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[126] Shannon Tiezzi, "China's Response to the US Cyber Espionage Charges," *The Diplomat*, May 21, 2014, accessed January 20, 2016, http://thediplomat.com/2014/05/chinas-response-to-the-us-cyber-espionage-charges/.

At the end of the year, in what *Fortune* called the "Hack of the Century," Sony Pictures endured a debilitating cyber attack that destroyed company networks and computers, embarrassingly detailed the inner workings of the company, exposed employee personal information, and nearly cancelled a movie.[127] The FBI would eventually implicate North Korea. During an end-of-the-year news conference, the president confirmed North Korea's involvement and the certainty of an eventual US response (the administration would impose economic sanctions in early January).[128] He also reinforced the fact that, since 2009, the administration had been working to improve cybersecurity but that more needed to be done, including international norms and Congressional action on cyber legislation particularly relating to information sharing.[129]

Both the PLA indictment and the response to the Sony hack would preview the administration's actions the next year.

2015

On January 13, the administration submitted another cyber-related legislative proposal, the first since 2011. Given the continued pace of threats and compromises, the proposal updated some of the 2011 provisions that Congress had yet to act on as well as added new language to improve information sharing. The proposal called for better private sector sharing with DHS, which would then share and coordinate with relevant federal agencies; creation of Information

[127] Peter Elkind, "Inside the Hack of the Century: Part 1," *Fortune*, July 1, 2015, accessed January 20, 2016, http://fortune.com/sony-hack-part-1/.

[128] White House, Office of the Press Secretary, *Statement by the Press Secretary on the Executive Order Entitled "Imposing Additional Sanctions with Respect to North Korea,"* January 2, 2015, accessed January 20, 2016, https://www.whitehouse.gov/the-press-office/2015/01/02/statement-press-secretary-executive-order-entitled-imposing-additional-s.

[129] White House, Office of the Press Secretary, *Remarks by the President in Year-End Press Conference*, December 19, 2014, accessed January 20, 2016, https://www.whitehouse.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference.

Sharing and Analysis Organizations (voluntary groups of private companies that would exchange information with one another and with the government); targeted liability protection for companies that shared information, contingent upon their compliance with privacy guidelines; modernized law enforcement authorities to combat cyber crime; and standardized federal law for data breach reporting.[130]

One month later at Stanford University, the president hosted the White House Summit on Cybersecurity and Consumer Protection. The summit—"a milestone in our Nation's efforts to strengthen its cyber defenses"[131]—brought together key leaders from government, industry, academia, and consumer advocate organizations. The summit highlighted recent successes (including the use of the Cybersecurity Framework by prominent businesses as well as the formation of several private sector information sharing organizations) but also served as another legislative call to action.[132] The president announced the stand-up of the Cyber Threat Intelligence Integration Center (a government clearinghouse for cyber threat information) and then ceremoniously signed Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing," which contained key elements of the administration's legislative proposal.

In April, the president signed Executive Order 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," which provided a framework for imposing economic sanctions against malicious cyber actors. While certainly the new order extended from the US response to North Korea's attack against Sony, it also seemed to

---

[130] White House, Office of the Press Secretary, *Securing Cyberspace: President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts*, January 13, 2015, accessed January 12, 2016, https://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat.

[131] White House, Office of the Press Secretary, *Remarks by the President at the Cybersecurity and Consumer Protection Summit*, February 13, 2015, accessed January 12, 2016, https://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.

[132] Ibid.

reflect the need for a new tool in combating cyber malfeasance. Lisa Monaco, the Assistant to the President for Homeland Security and Counterterrorism, said, "We need to deter malicious cyber activity and to impose costs in response to the most significant cyber intrusions and attacks, especially when those responsible try to hide behind international boundaries…we need a capability to deter and impose costs on those responsible for significant harmful cyber activity where it really hurts—at their bottom line."[133]

Two months later, OPM reported an extensive cyber breach that, ultimately, would involve the compromise of personal information for nearly 22 million citizens (government employees and contractors who had applied for security clearances since 2000—as well as their friends, relatives, and associates) and 1.1 million fingerprint records. While the administration did not specifically accuse China, the Director of National Intelligence implied as much.[134]

According to press reports, the scale of the OPM intrusion as well as growing political pressure to push back against China for currency manipulation, South China Sea claims, and other disputes, led the administration to consider imposing sanctions against Chinese companies and individuals suspected of economic espionage under the framework provided by the recent executive order. Such public reporting that sanctions were being considered likely was meant to signal US displeasure prior to Xi Jinping's visit to the United States in September.[135] In a flurry

---

[133] Lisa Monaco, "Expanding Our Ability to Combat Cyber Threats," White House blog, April 1, 2015, accessed January 20, 2016, https://www.whitehouse.gov/blog/2015/04/01/expanding-our-ability-combat-cyber-threats.

[134] Kristin Finklea, Michelle D. Christensen, Eric A. Fischer, Susan V. Lawrence, and Catherine A. Theohary, *Cyber Intrusion into US Office of Personnel Management: In Brief*, Congressional Research Service, July 17, 2015, 2, accessed January 12, 2016, http://digital.library.unt.edu/ark:/67531/metadc743551/m1/1/high_res_d/R44111_2015Jul17.pdf.

[135] Ellen Nakashima, "US Developing Sanctions Against China Over Cyberthefts," *Washington Post*, August 30, 2015, accessed January 10, 2016, https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html?mod=djemCIO_h; David Nakamura, "Tensions With China Loom Larger as Obama Prepares to Welcome Xi Jinping," *Washington Post*, August 12, 2015, accessed January 10, 2016, https://www.washingtonpost.com/news/post-politics/wp/2015/08/12/tensions-with-china-loom-

of activity before Xi's arrival, a Chinese delegation flew to Washington to discuss cyber issues and avert a public relations catastrophe.[136] In the end, both the United States and China got what they wanted: an agreement to normalize one of the most contentious issues between them while simultaneously saving face. After the summit, both leaders agreed on "timely responses" to investigate and stop malicious activity, that neither country would conduct cyber economic espionage, that they would work together to promote international norms, and that they would establish a formal dialogue as well as a hotline.[137] The first meeting between senior US and Chinese officials to hammer out details of the agreement occurred on December 1, with the next scheduled for June.[138]

The most prominent development in support of the president's cyber roadmap, however, occurred before the year would close, with the administration finally securing what had been a key policy objective since 2009 but which had been politically elusive. On December 18, the president signed the Cybersecurity Act of 2015.[139]

---

larger-as-obama-prepares-to-welcome-xi-jinping/.

[136] Shannon Tiezzi, "US, China Hold Cyber Talks Before Xi's Visit," *The Diplomat*, September 15, 2015, accessed January 13, 2016, http://thediplomat.com/2015/09/us-china-hold-cyber-talks-before-xis-visit/.

[137] White House, Office of the Press Secretary, *Fact Sheet: President Xi Jinping's State Visit to the United States*, September 25, 2015, accessed January 13, 2016, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

[138] Department of Homeland Security, Office of Public Affairs, *First US-China High-level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes*, December 2, 2015, accessed January 25, 2016, http://www.dhs.gov/news/2015/12/02/first-us-china-high-level-joint-dialogue-cybercrime-and-related-issues-summary.

[139] Title I, the Cybersecurity Information Sharing Act of 2015, permits companies to monitor and voluntarily share information with each other and the federal government, so long as irrelevant personal information is scrubbed. Companies are generally shielded from liability and antitrust laws, consistent with their adherence to safeguards designed to protect individual privacy or prevent market collusion. While information sharing remains voluntary, "many companies…view liability protection as a minimum requirement to take part in any information-sharing arrangement." Additionally, the act allows the government to share classified information with appropriately cleared portions of the private sector. See *Cybersecurity Nexus Special Report: US Enacts Cybersecurity Information Sharing Legislation* (Rolling Meadows, IL: ISACA,

Impediments to action

Clearly, there had been a gathering recognition and more vocal US response over the course of the administration. Yet if Chinese cyber economic espionage and theft of intellectual property was regarded as such a significant threat—which the administration and others had claimed it to be—why did it take so long to pass legislation aimed at improving the nation's ability to contend with malicious actors in cyberspace?

Kissinger, in *World Order*, describes the advent of cyberspace (and related technology) as a singular epoch. Whereas previous technological revolutions were slowly embraced and integrated over time, the Information Age had been distinct. "Cyberspace challenges all historical experience."[140] Cyberspace creates novelty: what can be done with it, and what can be done to it.

During his remarks at the Cybersecurity and Consumer Protection Summit in February 2015, the president acknowledged the general difficulty in better securing cyberspace. "Some of the challenges I've described today"—the character of cyberspace that brings opportunities but also threats, the shared responsibility between government and the private sector to protect networks and information, the need to quickly adapt, the requirement to protect privacy and civil liberties—"have defied solutions for years."[141]

Overlaid on top of that experiential and philosophical tension, the influence of Congress, the private sector, and the public have shaped the US response.

January 6, 2016), 3, 6, accessed January 10, 2016, http://www.isaca.org/cyber/Documents/CSX-Special-Report_misc_Eng_0116.pdf.

[140] Kissinger, *World Order*, 344.

[141] White House, Office of the Press Secretary, *Remarks by the President at the Cybersecurity Summit*.

Congress

The administration's difficulty in securing significant cyber legislation is partially explained by what confounds all presidents: domestic politics and the role of competing interests between various stakeholders and audiences. Until the waning days of 2015—and despite the apparent threat and impact posed by Chinese cyber economic espionage (not to mention the more often heard "cyber Pearl Harbor" and "cyber 9/11" narratives that dominated media reporting)—Congress had not passed substantial cyber legislation since 2002.[142]

Within the context of local, state, and national politics, implementing and amending laws would be additionally challenged by the character of cyberspace—a virtual world beset with technical complexity and rapid change—at the same time that it became essentially woven into the fabric of everyday life. A democratic, legislative process designed in the 18th century would necessarily lag behind the technology of the 21st. For example, a 2013 Congressional Research Service survey found more than 50 laws with potential applicability to cybersecurity.[143] Changing such a vast scope of laws—or attempting to condense them into fewer yet more authoritative statutes—would be difficult and filled with political and philosophical tension.

Central to the debate was the role of government, the likelihood of bureaucratic growth and meddling, imposition of burdensome costs on the private sector, the potential for corporate influence in developing and enforcing standards and policies,[144] and preserving individual privacy and civil liberties.[145] Within that context, legislative action would need to strike a balance to

[142] Eric A. Fischer, *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*, Congressional Research Service, June 20, 2013, 3, accessed February 2, 2016, http://digital.library.unt.edu/ark:/67531/metadc227741/m1/1/high_res_d/R42114_2013Jun20.pdf.

[143] Ibid., 20.

[144] Fischer, *Federal Laws Relating to Cybersecurity*, 38.

[145] Particularly with the outcry over government surveillance and concerns for misuse of collected information, privacy and civil rights advocacy groups have routinely attempted to prevent legislation that would enable public-private information sharing without judicial

accommodate multiple perspectives and limit the effect of unintended consequences, while simultaneously avoiding the most contentious prospect of all: undercutting the Constitution and harming very fundamental American values.

Legislation would need to overcome existing statutes that inhibited much of the actions needed to improve cybersecurity, but in a way that would help solve the problem without exacerbating it or creating new ones. For instance, incentivizing the private sector to voluntarily share information with the government would likely require amending the Freedom of Information Act to prevent the exposure of corporate secrets, yet such a change would also "prompt concerns about decreases in federal transparency."[146] Enabling companies to share information with each other to exchange cyber threat data or best practices would run counter to anti-trust laws designed to ensure competitive, fair, and free markets.[147] Collection and analysis of certain personally identifiable information (such as network and computer information) to support cyber incident response or threat mitigation would mean changing the Privacy Act of 1974 at the risk of potentially "compromis[ing] the protection provided by the act."[148] Sharing classified information with the private sector would require more security clearances, impose

oversight. See Eliza Sweren-Becker, "Congress Working in the Dark on Cybersecurity Bill," American Civil Liberties Union blog, November 17, 2015, accessed January 25, 2016, https://www.aclu.org/blog/free-future/congress-working-dark-cybersecurity-bill; "Cybersecurity Privacy Practical Implications," Electronic Privacy Information Center, accessed January 25, 2016, https://epic.org/privacy/cybersecurity/#articles; "OTI Deeply Disappointed About Passage of Dangerous Cybersecurity Bill," Open Technology Institute, December 18, 2015, accessed January 25, 2016, https://www.newamerica.org/oti/oti-deeply-disappointed-about-passage-of-dangerous-cybersecurity-bill/. Various attempts at legislation sought to strike a balance between privacy and security but ultimately failed, at least until the well-publicized breaches in 2014 and 2015 "jump-started" legislative action and Congress and the president were able to find a compromise solution. See Elias Groll, "A Cybersecurity Bill Light on Security, Heavy on Corporate Protection," *Foreign Policy*, September 14, 2015, accessed January 25, 2016, http://foreignpolicy.com/2015/09/14/a-cybersecurity-bill-light-on-security-heavy-on-corporate-protection/.

[146] Fischer, *Federal Laws Relating to Cybersecurity*, 30.

[147] Fischer, *Federal Laws Relating to Cybersecurity*, 23-24.

[148] Ibid., 32.

investigative and financial costs, and increase the potential for the unauthorized disclosure of national security information.[149] Because of "interconnectivity" between a web of laws, changing one would likely mean having to change many.[150]

Given the difficultly, then, of orchestrating legislative solutions, the administration sought to address cybersecurity through executive action, which could impact federal agencies but not necessarily the nation as a whole. The private sector—the businesses most vulnerable to cyber intrusions from an economic standpoint—could only be encouraged, with few incentives, to participate on a voluntary basis, as the NIST Cybersecurity Framework attempted to do. But such an incremental approach seemed to have little impact in deterring or stopping threats. By 2013, the cacophony of voices calling for whole-of-government traction appeared to reach a crescendo. The IP Commission highlighted the ineffectiveness of existing US policies and pressed for "robust and swift action"[151] and "urgent consideration"[152] of policy and legislative recommendations. McConnell, Chertoff, and Lynn wrote that "cyber 'economic espionage' looms even more ominously" than attacks against critical infrastructure.[153] The Defense Science Board report said that "[t]he long term loss of so much intellectual property and capability will result in a serious competitive disadvantage to the US economy."[154] General (ret.) Michael Hayden, former NSA and CIA Director, was pointed. In an opinion piece, he criticized the administration for cyber policy that represented the path of least resistance. Instead of developing national

[149] Ibid., 27.

[150] Ibid., 50.

[151] Commission on the Theft of American Intellectual Property, 21.

[152] Ibid., 2.

[153] McConnell, Chertoff, and Lynn.

[154] DOD Defense Science Board, *Task Force Report*, 31.

consensus and making "hard decisions" through dialogue and discussion, the administration refused to "spill the domestic political blood" necessary to do so.[155]

The administration failed to propose cybersecurity legislation when it would have had the greatest chance of legislative success during the 111th Congress, with both houses controlled by the Democrats. Arguably, other domestic and international imperatives (shoring up the economy, dealing with the wars in Iraq and Afghanistan, pushing for health care reform) consumed the policymaking agenda. The nexus between an evolving domain and its relationship to Chinese economic espionage would be partially masked by competing policy priorities as well as a lack of evidence that, at least publicly, didn't connect the dots. As time went on, particularly with a growing number of reports about the threat and cost, legislation was trapped in the polarizing partisanship of divided government. The caustic relationship between the executive and legislative branches during the 112th and 113th Congresses—highlighted with debt ceiling debates, government shutdowns, and sequestration—prevented bipartisan compromise on many issues, let alone one that was by its nature contentious given divergent views on such things as the role of government and privacy. And so it is ironic that success would be found during the 114th Congress, with both houses Republican, and the president, presumably, at his politically weakest point.

The fact that the Cybersecurity Act of 2015 was attached to the spending omnibus at the end of the year largely guaranteed its passage. For the Republicans and Democrats in both houses to agree to such a legislative technique after years of bickering about cybersecurity infers that the gathering threat had reached a crescendo, and that consensus on doing something, despite howls from privacy advocates and big government alarmists, trumped partisan instinct. Much of the

[155] Michael V. Hayden, "Have the Courage to Deal With Cyber War," CNN, February 19, 2013, accessed January 13, 2016, http://edition.cnn.com/2013/02/19/opinion/hayden-courage-security-decisions/index.html.

debate in support of legislation outlined the long history of inaction in the face of a metronome of increasingly serious cyber intrusions and vulnerabilities, and harkened to a September 10th moment: the nation was poised to suffer because of a failure to respond in the face of a growing threat.[156] In the lead-up to final passage, both chambers had voted with broad bipartisan support on three cybersecurity resolutions (two in the House and one in the Senate).[157] The December passage of the Consolidated Appropriations Act of 2016 (to which the cybersecurity legislation was attached) similarly passed with bipartisan support.

Corporate America

At the same time the administration and Congress wrestled with the confluence of cybersecurity and economic espionage, the private sector faced difficulties in orienting to the problem—and likely contributed to the delays in seeking an effective "whole-of-nation" response.[158]

Cyberspace makes it easy to infiltrate and steal, but it also makes it difficult to detect. Nation-state cyber actors, owing to the vast technical resources at their disposal, face "relatively

[156] See Senators Dianne Feinstein of California and Susan Collins of Maine, speaking for the Cybersecurity Information Sharing Act of 2015, S.754, on August 5, 2015, to the Senate, 114th Cong., 1st sess., *Cong. Rec.* 161, no. 126: S6329-S6331, S6337.

[157] HR 1560, Protecting Cyber Networks Act, passed on April 22, 2015, 307 to 116. HR 1731, National Cybersecurity Protection Advancement Act of 2015, passed on April 23, 2015, 355 to 63. S.754, Cybersecurity Information Sharing Act of 2015, passed on October 27, 2015, 74 to 21. See *Final Vote Results for Roll Call 170,* Office of the Clerk, US House, April 22, 2015, accessed January 29, 2016, http://clerk.house.gov/evs/2015/roll170.xml; *Final Vote Results for Roll Call 173,* Office of the Clerk, US House, April 23, 2015, accessed January 29, 2016, http://clerk.house.gov/evs/2015/roll173.xml; *Roll Call Vote 291,* US Senate, October 27, 2015, accessed January 29, 2016, http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=114&session=1&vote=00291.

[158] Corporate interests certainly shaped government response and inhibited a more direct approach, as they had since the 1990s. "US business interests in the China market grew markedly in 1992, and were credited with playing an important role in convincing the Clinton administration in 1994 to stop linking US most-favored-nation trade treatment to improvements in China's still poor human rights conditions." Sutter, *China's Rise,* 44.

little risk of detection by their private sector targets."[159] And even if an intrusion is detected, determining who is responsible is masked by difficulties in attribution. Given the ability to cleverly route an attack through innumerable hop points geographically bounded only by the world, using proxies (both technically, as in compromised computers, and organizationally, by using hacker groups), and employing difficult to detect tools (unknown malware or vulnerability exploits), an attacker has the advantage.[160] According to General Keith Alexander, during a 2012 speech at the American Enterprise Institute, for every company that knows it's been hacked, "more than a hundred" don't.[161]

Add to that, when companies are able to discover an intrusion, such awareness often lags by months. In its 2013 report, Mandiant suggests an average 243-day flash-to-bang. The 2011 Office of the National Counterintelligence Executive report is more dramatic: "Many victims of economic espionage are unaware of the crime until years after loss of the information."[162]

At the same time, network security as well as cyber attacks are by definition technical in nature. That technological complexity creates tension.[163] Corporate leadership unable or unwilling to actively engage in or resource technical efforts fosters organizational weakness in

---

[159] Office of the National Counterintelligence Executive, i.

[160] Ibid.

[161] Keith Alexander, "Cybersecurity and American Power: Addressing New Threats to America's Economy and Military" (video of speech, American Enterprise Institute, Washington, DC, July 9, 2012), accessed January 8, 2016, https://www.aei.org/events/cybersecurity-and-american-power/. While his anecdote may be apocryphal, it does point to the difficulty of knowing when an electronic burglar has successfully intruded, even for the most technologically advanced corporations.

[162] Office of the National Counterintelligence Executive, 3.

[163] See Andrea Peterson's account of the Internet dust-up when Michael Daniel, the president's cybersecurity coordinator, proclaimed that it was better for him not to be a techno-nerd. Andrea Peterson, "Does the White House's Cybersecurity Czar Need to be a Coder? He Says No," *The Switch* (blog), *Washington Post*, August 22, 2014, accessed January 12, 2016, https://www.washingtonpost.com/news/the-switch/wp/2014/08/22/does-the-white-houses-cybersecurity-czar-need-to-be-a-coder-he-says-no/.

the face of determined cyber adversaries.[164] As a result, many companies are likely ill-prepared to not only defend their critical data but also identify what requires defending in the first place.[165]

The dilemma of not knowing when an attack has occurred coupled with the oftentimes arcane nature of network technology is exacerbated by the fact that network security costs money. Particularly as cyberspace has evolved, security has become a priority to the extent that a company has assessed the risk as outweighing the cost. Yet even suffering an attack might not result in reposturing or additional investment.

Broadly, companies don't necessarily have the financial incentive to spend more to protect corporate or customer information. Benjamin Dean, in an analysis of high-profile data breaches at large companies, showed that financial losses were "typically less than 1% of a company's annual sales."[166] Given the cost to shore up information security beforehand or simply absorb a "rounding error" afterwards[167], many companies have "made the calculation that they can mitigate the risk or absorb the lost revenues and profits."[168] Yet the costs of fixing cyber attacks, after the fact, have steadily increased.[169]

---

[164] Office of the National Counterintelligence Executive, A-2. The report highlights lack of involvement by corporate management with network security matters as a contributing factor to economic espionage vulnerability.

[165] *CSIS/DOJ Active Cyber Defense Experts Roundtable*, Center for Strategic and International Studies and Cybersecurity Unit, Department of Justice, March 10, 2015, 5, accessed October 10, 2015, http://csis.org/files/publication/150519_CountermeasuresDOJ.pdf.

[166] Benjamin Dean, "Why Companies Have Little Incentive to Invest in Cybersecurity," Conversation.com, March 4, 2015, accessed January 29, 2016, http://theconversation.com/why-companies-have-little-incentive-to-invest-in-cybersecurity-37570. Insurance and tax-breaks help compensate.

[167] Erik Sherman, "The Reason Companies Don't Fix Cybersecurity," CBS Moneywatch, March 12, 2015, accessed January 29, 2016, http://www.cbsnews.com/news/the-reason-companies-dont-fix-cybersecurity/.

[168] Commission on the Theft of American Intellectual Property, 21.

[169] For an informative study on costs, see Ponemon Institute, *2015 Cost of Cyber Crime Study: United States* (Traverse City, MI: Ponemon Institute, October 2015), accessed January 29, 2016, https://ssl.www8.hp.com/ ww/en/secure/pdf/4aa5-5208enw.pdf.

Once a compromise has occurred, businesses face few, but nonetheless consequential, options. Rightfully focused on the bottom-line, a company may weigh the decision on whether to seek outside help or notify shareholders, customers, or the public at large based on the potential impact to the health of the business. Unfortunately, "[m]any companies are unaware when their sensitive data is pilfered, and those that find out are often reluctant to report the loss."[170]

According to the IP Commission, businesses that end up staying quiet do so because of the "reputational effects" public exposure would create, and, if the cyber theft originates from a "strategically important market," it may be more cost-effective in the long run to ignore it.[171] Put another way, businesses may not want to accuse a foreign government for fear of reducing market share or profit potential.[172]

Which is particularly problematic when it has come to the vastness of the Chinese market. Globalization and the great outsourcing rush of the 1990s—fueled by corporate desire for maximized profits and consumer desire for minimized prices—possessed, in the background, the notion that one day China's masses would no longer be economically developing but would instead have the capital for economic spending. China's 11th Five Year Plan presaged as much. Portions of Corporate America, perhaps because of its already significant investment in China and because of the allure of future possibility, became blind to what was happening to it by the country that offered it so much potential.[173]

---

[170] Office of the National Counterintelligence Executive, i.

[171] Commission on the Theft of American Intellectual Property, 23.

[172] Office of the National Counterintelligence Executive, 3.

[173] See Danchev, "Google-China Cyber Espionage Saga." After the 2010 Google hack, other large American IT companies seemed to dispense with notions of widespread Chinese economic espionage as a threat to corporate interests because of their stake in the Chinese market. Also, see Gross, "Operation Shady Rat." After the Operation Shady RAT report was released, McAfee apparently offered to help many of the targeted companies; most refused or ignored the requests, seemingly out of denial or for fear of angering the Chinese government.

And so a mix of complicating factors—reputation, profits, obscure technology, hidden vulnerabilities, masked threats—served to insulate the private sector from the fleecing it had endured. Only now, it seems, are businesses paying heed to the McConnell, Chertoff, and Lynn admonishment in 2012. "Corporate America must do its part, too. If we are to ever understand the extent and impact of cyber espionage, companies must be more open and aggressive about identifying, acknowledging and reporting cyber theft incidents."[174]

Narratives

The fact that retired government officials, in 2012, felt compelled to reach out to the American people to address the relationship between cyberspace and economic espionage speaks to another problem. In the absence of a specific government effort to simultaneously explain the issue and spur action, informed private citizens found it their duty to go public. Alternatively, they went public on behalf of the government. In either case, the administration's approach was indirect.

The administration's relative silence was occasionally interrupted by calls to action and calls for change. Yet, specific to Chinese cyber economic espionage, including the 2014 indictments, the US government had really only waved its finger (oftentimes ambiguously) with little effect. According to the 2013 report from the IP Commission, while the "United States has attempted to hector China…into doing a better job of protecting IP,"[175] the fact remains that "theft is increasing, and cyber-enabled forms, in particular, are proving ever more deleterious."[176]

Why, then, limit the official response to nagging or third party outings?

[174] McConnell, Chertoff, and Lynn.

[175] Commission on the Theft of American Intellectual Property, 20.

[176] Ibid, 21.

Martin Libicki, in *Crisis and Escalation in Cyberspace*, provides insights into how a state can orient and respond to what it perceives as harmful cyber activity. While his premise, as the title implies, relates to managing cyber crises, it also underscores some of the difficulties the United States has faced (or created) in responding to Chinese cyber economic espionage.

According to Libicki, cyber crises can be generally managed like other types of political and military crises. Yet while there are similarities, he also highlights caveats based on the unique nature of cyberspace, in that it "has created new ways to stumble into war."[177] The novelty of cyberspace and the features of events within it—uncertainty about whether something happened or how serious it may be, who may have done it and with what intentions—can present real or imagined problems that may lead to or exacerbate a crisis.[178]

An element of his argument suggests that cyberspace owes its ambiguity, in part, because its reality—to the extent that it is known—belongs to national security structures. "Everything is done in great secrecy, so what one state does must be inferred and interpreted by others."[179] A critical factor, therefore, of crises in cyberspace relates to the role of narratives and signals.

"Narratives are made up of the stories that people, organizations, and states tell about themselves to others as a way of putting events in a broader and consistent context and justifying their attitudes and actions."[180] Particularly because cyberspace as a domain continues to evolve, and, as Kissinger said, is ahistorical and therefore novel, actions in it "demand a narrative."[181] A state may have a number of narratives depending upon context—its "self-chosen status as a

[177] Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica, CA: RAND, 2012), 123.

[178] Ibid., 145.

[179] Ibid.

[180] Libicki, *Crisis and Escalation*, xiv.

[181] Ibid., 39.

victim, an accuser, a retaliator, or an aggressor"[182]—that help explain how it views cyberspace and events within it, and serves to guide how it reacts internationally and domestically.

Whereas narratives are broad in terms of message and audience, signals are more specific and convey seriousness. "Signals…supplant or supplement words with deeds."[183] Signals are designed to influence adversary behavior by indicating the degree of displeasure or exacting a cost in reaction to an event, and they fall within a spectrum based on "what a state has claimed as its due" in cyberspace[184]—its narrative. A signal too strong may box a state into a corner; a signal too weak may imply "there is nothing about which to be resolute."[185]

Effective narratives, then, ought to be open and explanatory and designed to garner support or explain action. Signals may be publicly visible or hidden from public view, but must be properly received and interpreted by the intended audience.[186]

From a narrative standpoint, the United States has found it difficult to explain its position in a way that catalyzes action. Internationally, it offered its international strategy in 2011 to describe how the United States viewed cyberspace—with particularly American notions of ideals and values. But problems associated with lack of international legal norms, diverging views between "traditional" espionage and "economic" espionage, and credibility perceptions (especially post-Snowden), served China's purposes instead.

Domestically, the narrative lacked official vigor. Following its 2009 cyberspace policy review, it took until 2011 before the administration attempted to shape the narrative—manifested

[182] Ibid., 45.

[183] Ibid., xv.

[184] Ibid., 67.

[185] Ibid., 68.

[186] Ibid., 62.

by the international strategy, cybersecurity legislative proposal, and Office of National Counterintelligence Executive report.[187]

For all of the president's State of the Union addresses between 2010-2016, the Internet was addressed 13 times (mostly relating to innovation, infrastructure, and terrorism); China, 17 (typically regarding trade, unfair trading practices, and clean energy); and cybersecurity, 6 (but not until 2012 and none in 2016).[188] There was one mention of cyber-enabled corporate secret theft in 2013 (but not linked to China), the same year the administration attempted to become more assertive with Chinese leadership (Donilon's speech at the Asia New York Society, Hagel's speech in Singapore, the president's summit with Xi Jinping) until competing post-Snowden narratives muted the US position.

Beyond those pointed attempts, the narrative was largely hinting, rarely specific, and left much to the imagination. The 2013 *Administration's Strategy on Mitigating the Theft of US Trade Secrets* is illustrative. Of eight callout boxes designed to show real world examples of trade theft, six highlighted China—but without any announced finding.[189] In an annex that summarized Department of Justice trade secret theft cases between January 2009 and January 2013, 17 of the 20 were related to China—but again without any judgment.[190] In another annex, a 2012 report demonstrating trends of foreign collection of US defense industry technology, the Defense Security Service went out of its way to avoid calling a duck a duck: throughout the report, it regionalized the threat and referred euphemistically to actors in "East Asia and the Pacific" as the

[187] In their 2012 editorial, McConnell, Chertoff, and Lynn reference that report and suggest government knowledge of the extent of Chinese actions at least two years prior.

[188] See "Bibliography" for White House, Office of the Press Secretary, *State of the Union* citations.

[189] White House, *Administration Strategy on Mitigating the Theft of US Trade Secrets*, February 2013, 4, 5, 7, 9, 10, accessed January 22, 2016, https://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_us_trade_secrets.pdf.

[190] White House, *Administration Strategy on Mitigating*, Annex B, "Summary of Department of Justice Trade Secret Theft Cases."

"preeminent attempted collectors."[191] In all of those cases, the narrative failed to draw necessary conclusions and instead left it to the interpretation of whatever audience was paying attention.

Which underscores another problem. To the extent that the narrative was publicly offered, it often was isolated to stovepiped channels of communication focused on who was interested as opposed to who should be. Put another way, attempts to shape the narrative through think tank speeches, foreign policy journals, Sunday morning talk shows, press conferences, and Congressional testimony targeted policy elites, intellectuals, and other presumptive influencers—not the broader public.

Private cybersecurity firms, seemingly, became impatient with a government obviously staring at the facts but apparently unwilling to announce them. Mandiant, which released the 2013 report detailing PLA Unit 61398, said:

> It is time to acknowledge the threat is originating in China, and we wanted to do our part to arm and prepare security professionals to combat that threat effectively. The issue of attribution has always been a missing link in publicly understanding the landscape of [Advanced Persistent Threat] cyber espionage. Without establishing a solid connection to China, there will always be room for observers to dismiss APT actions as uncoordinated, solely criminal in nature, or peripheral to larger national security and global economic concerns.[192]

If Libicki is correct in his assertion that cyberspace begs for a government narrative that provides clarity, how clear is the message of Chinese cyber economic espionage when the details are delivered by the private sector?

Perhaps Libicki is also correct when he suggests that, "as hard as it is to teach leaders about the facts and issues involved in cyberattacks, teaching the public is harder still."[193]

---

[191] Ibid., Annex D, "2012 DOD Defense Security Service Report," 64.

[192] Mandiant, *APT1*, 6. McAfee, as well, highlighted in its 2011 report on Operation Shady RAT a lack of public awareness and "understanding of this significant national security threat." Alperovitch, *Operation Shady RAT*, 3.

[193] Libicki, *Crisis and Escalation*, 10.

Ambiguity may be a condition as opposed to a wanting strategy.[194] The 2009 cyberspace policy review, invoking the national mood after the 1957 Sputnik launch, said that government and industry "should explain this challenge [cybersecurity]" so as to garner popular support for action.[195] Yet the recommendations for increasing public awareness were limited to "public service announcement"-like campaigns focused on online safety, or highlighting the need for science, technology, engineering, and math education to encourage the next generation of the IT workforce.[196]

The domestic narrative falls apart when the message by design of its transmission is delivered only to a portion of the public—leaving the rest to do better at protecting themselves online despite the anesthetizing effect of repeated widespread data breaches, with statistics that numb precisely because they are so harrowing yet commonplace—and when the government weakly generalizes so as to leave the threat undifferentiated.

From a signaling standpoint, the United States appears equally as challenged as it has been with its narrative.

The public signals to China increased in scope and frequency over time.[197] While this may be attributable to the administration's growing recognition of the problem and eventually having had enough—more robust and periodic signals representing firmness of position and will—the fact that incrementally more direct signaling was required suggests something else. According to Libicki, "The efficacy of signaling depends, in large part, on its acceptance of

---

[194] Libicki also notes that time lags (despite the speed-of-light nature of cyberspace) dampen emotions. Whereas a kinetic attack against Iranian nuclear facilities would immediately arouse public sentiment, Stuxnet, because it played out over the course of months, limited public outcry. Libicki, *Crisis and Escalation*, 10.

[195] White House, *Cyberspace Policy Review*, iv.

[196] Ibid., 13-15.

[197] See "Chronology" section.

something *as* a signal."[198] Beyond that, signaling ought to bear gravity. "Talk is cheap and, being cheap, may not be taken seriously."[199] And it is this last condition that is most troubling for predatory cyber economic espionage behavior.

The fact that US signals had to be repeated more strenuously implies that the signal was not properly received or, more likely, simply ignored. A significant example is the relationship between the overt signaling of the 2014 indictments of the PLA officers and the hinted threat of sanctions (enabled by last year's executive order) prior to the 2015 Obama-Xi summit that led to the cyber agreement between the United States and China. According to James Lewis of the Center for Strategic and International Studies, "[T]he Chinese hated the indictments, and the experience of indictments reinforced the potential of US sanctions in ways that helped the US and China reach agreement on cybersecurity."[200] Reinforcing signals aside, the distance between them implies that the first signal wasn't firm enough to prevent the need for the second. Put another way, despite the perceived strength of the 2014 US signal, unacceptable Chinese behavior continued.[201]

---

[198] Libicki, *Crisis and Escalation*, 62.

[199] Ibid., 63.

[200] James A. Lewis, "Cyber War: Definitions, Deterrence, and Foreign Policy," statement before the House Committee on Foreign Affairs, September 30, 2015, 6, accessed January 12, 2016, http://csis.org/files/attachments/ts150930_Lewis.pdf.

[201] With respect to the 2015 bilateral agreement, past is prologue. CrowdStrike, a cybersecurity firm, suggested in October that Chinese efforts to steal US intellectual property continued despite the September agreement. In November, the Director of the National Counterintelligence and Security Center indicated that nothing, really, had changed. See Associated Press, "China Already Violating US Cyberagreement, Group Says," CBS News, October 19, 2015, accessed January 25, 2016, http://www.cbsnews.com/news/crowdstrike-china-violating-cyberagreement-us-cyberespionage-intellectual-property/; Mark Hosenball, "US Counterintelligence Chief Skeptical China has Curbed Spying on US," Reuters, November 18, 2015, accessed January 25, 2016, http://www.reuters.com/article/us-usa-cybersecurity-idUSKCN0T72XG20151119.

According to Lewis, "so far, our opponents have faced no cost and little risk in carrying out malicious cyber actions."[202] Libicki points to the underlying problem. "States get into trouble…by not responding to salami tactics."[203] Consistent US finger-wagging, with no real follow-through, enabled China to continue its massive plundering with slight pauses only when the United States upped the ante by figuratively slapping its hand.

Signals lack credibility when they don't accrue a more durable cost;[204] incredible signals undermine the target state by reinforcing the behavior of the attacking state. "In some circumstances, forgoing a vigorous response may create a new baseline for misbehavior in cyberspace. If the target state has advocated a standard for behavior and accepts the incident without too much protest, it signals a lack of seriousness in general, not just about cyberspace. The attacker and other states may read the failure to respond as evidence of weakness."[205]

An incomplete narrative that fails to cultivate support internationally or domestically, coupled with signals that fail to convey enough seriousness to change the cost-benefit calculation, defy Libicki's notion that, in cyberspace, "a state that would prevail has to make a clear story."[206]

Conclusion

The story, then, of China's efforts to steal American intellectual property through cyberspace is a chronicle of opportunity, both gained and lost.

On the one hand, China—armed with a national purpose, effective narrative, and well-articulated and planned strategic goals—viewed its rise as inevitable but dependent upon necessary conditions, particularly a peaceful regional and international climate that would allow it

[202] Lewis, "Cyber War," 5.

[203] Libicki, *Crisis and Escalation*, 68.

[204] Ibid., xv.

[205] Ibid., 11.

[206] Ibid., 17.

to grow and gather. Conditions, being temporary, underscored the two-fold need to prevent or blunt US counterbalancing as well as to seize the initiative, especially as the pressures of rising popular expectations and unsustainable economic growth could undermine the imperatives of Party legitimacy and national ambitions. Imperatives, being urgent, highlighted speed in the quest for innovation, economic transformation, and global competitiveness. And so cheating—manifested through a sense of urgency and enabled by a connected world—became state policy. Regardless of moral or ethical judgments (which, from a realist perspective, are largely irrelevant in international relations), opportunity grasped in self-interest is still opportunity grasped.

On the other hand, the United States seemed unmotivated to deny the opportunities China sought at the expense of America's long-term economic wellbeing. Despite the consistency of the administration's cybersecurity objectives, it was by turns lurching for solutions but also shying away from them. Certainly cybersecurity garnered executive and legislative effort. Numerous Congressional committees and subcommittees held hearings, federal agencies developed capabilities and organizations, and the administration implemented policies and strategies in an attempt to shore up the nation's defenses. Yet there is little accounting of a clear, purposeful effort to directly confront China about cyber economic espionage, make it too politically or economically costly for it to bear, or galvanize public support.

Perhaps the lack of clarity was pragmatic. To a degree, accommodating China instead of antagonizing it would reduce the likelihood of conflict (cyber or otherwise), potentially moderate its behavior to ensure its integration as a contributing member of the US-dominated international order, and keep open to American businesses the future of a brimming market. Given the stakes of the world's most important relationship to global stability, the opportunity costs of holding China too accountable for its actions, within the context of other international and domestic imperatives, could be too high. Alternatively, perhaps ambiguity was the result of plodding consistency. Having developed by May 2009 a cybersecurity agenda (related by definition to

cyber economic espionage), the administration stayed the course, with periodic deviations that returned to normal once circumstances settled down. The timeline of the administration's exertions is suggestive: seven months to appoint a cybersecurity coordinator, two years to unveil a legislative proposal and international cyberspace strategy, four years to issue a trade secret theft strategy and cyber-related executive order, and nearly seven years to sign a comprehensive cybersecurity bill—all while, apparently, China's stealing continued unabated.

On China's peaceful rise, Zheng Bijian proselytized, "What is therefore the United States to worry about?"[207] To the extent that the United States has been successful in preserving its economic security, which undergirds its power and position, perhaps not much. Yet to the extent that China's rise has been underwritten by the unconstrained theft of US intellectual property, perhaps the China dream may become America's nightmare.

[207] Zheng, *China's Peaceful Rise*, 8.

Bibliography

Alexander, Keith. “Cybersecurity and American Power: Addressing New Threats to America’s Economy and Military.” Video of speech, American Enterprise Institute, Washington, DC, July 9, 2012. Accessed January 8, 2016. https://www.aei.org/events/cybersecurity-and-american-power/.

Alperovitch, Dmitri. *Revealed: Operation Shady RAT: White Paper Version 1.1*. Santa Clara, CA: McAfee, 2011. Accessed January 13, 2016. http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

Art, Robert J. “The United States and the Rise of China: Implications for the Long Haul.” In Ross and Zhu, 260-290.

Carlson, Benjamin. “The World According to Xi Jinping.” *The Atlantic*, September 21, 2015. Accessed April 1, 2016. http://www.theatlantic.com/international/archive/2015/09/xi-jinping-china-book-chinese-dream/406387/#article-comments.

Center for Strategic and International Studies. “Significant Cyber Incidents Since 2006.” Washington, DC: Center for Strategic and International Studies. Accessed November 30, 2015. http://csis.org/files/publication/160406_Significant_Cyber_Events_List.pdf.

Chien, Eric and Gavin O’Gorman. *The Nitro Attacks: Stealing Secrets from the Chemical Industry*. Mountain View, CA: Symantec, 2011. Accessed January 14, 2016. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf.

Clegg, Jenny. *China’s Global Strategy Towards a Multipolar World*. New York: Pluto Press, 2009.

Clinton, Hillary Rodham. “Remarks on Internet Freedom.” Newseum, Washington, DC, January 21, 2010. Accessed January 15, 2016. http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

Commission on the Theft of American Intellectual Property. *The IP Commission Report.* N.p.: National Bureau of Asian Research, May 2013. Accessed November 20, 2015. http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

Consonery, Nicholas. “Testimony before the US-China Economic and Security Review Commission.” Prepared statement presented to US-China Economic and Security Review Commission, April 22, 2015. In US-China Economic and Security Review Commission, *China Ahead of the 13th Five-Year Plan*, 31-39.

CSIS/DOJ Active Cyber Defense Experts Roundtable. Center for Strategic and International Studies and Cybersecurity Unit, Department of Justice, March 10, 2015. Accessed October 10, 2015. http://csis.org/files/publication/150519_CountermeasuresDOJ.pdf.

Danchev, Dancho. “Google-China Cyber Espionage Saga: FAQ.” ZDNet, January 19, 2010. Accessed January 16, 2016. http://www.zdnet.com/article/google-china-cyber-espionage-saga-faq/.

Donilon, Thomas. “The United States and the Asia-Pacific in 2013.” Asia Society New York, March 11, 2013. Accessed January 8, 2016. http://asiasociety.org/new-york/complete-transcript-thomas-donilon-asia-society-new-york.

Drummond, David. “A New Approach to China.” Google Official Blog, January 12, 2010.

Accessed January 15, 2016. https://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

Elkind, Peter. “Inside the Hack of the Century: Part 1.” *Fortune*, July 1, 2015. Accessed January 20, 2016. http://fortune.com/sony-hack-part-1/.

Espinel, Victoria. “Launch of the Administration’s Strategy to Mitigate the Theft of US Trade Secrets.” White House blog, February 20, 2013. Accessed January 22, 2016. https://www.whitehouse.gov/blog/2013/02/20/launch-administration-s-strategy-mitigate-theft-us-trade-secrets.

Finklea, Kristin, Michelle D. Christensen, Eric A. Fischer, Susan V. Lawrence, and Catherine A. Theohary. *Cyber Intrusion into US Office of Personnel Management: In Brief*. Washington, DC: Congressional Research Service, July 17, 2015. Accessed January 12, 2016. http://digital.library.unt.edu/ark:/67531/metadc743551/m1/1/high_res_d/R44111_2015Jul17.pdf.

Fischer, Eric A. *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*. Washington, DC: Congressional Research Service, June 20, 2013. Accessed February 2, 2016. http://digital.library.unt.edu/ark:/67531/metadc227741/m1/1/high_res_d/R42114_2013Jun20.pdf.

Goldstein, Avery. “Parsing China’s Rise: International Circumstances and National Attributes.” In Ross and Zhu, 55-86.

Gross, Michael Joseph. “Enter the Cyber-dragon.” *Vanity Fair*, August 31, 2011. Accessed January 13, 2016. http://www.vanityfair.com/news/2011/09/chinese-hacking-201109.

Gross, Michael Joseph. “Exclusive: Operation Shady Rat—Unprecedented Cyber-espionage Campaign and Intellectual-Property Bonanza.” *Vanity Fair*, August 31, 2011. Accessed January 13, 2016. http://www.vanityfair.com/news/2011/09/operation-shady-rat-201109.

Harris, Shane. “Exclusive: Inside the FBI’s Fight Against Chinese Cyber-Espionage.” *Foreign Policy*, May 27, 2014. Accessed November 2015. http://foreignpolicy.com/2014/05/27/exclusive-inside-the-fbis-fight-against-chinese-cyber-espionage/.

Hayden, Michael V. “Have the Courage to Deal with Cyber War.” CNN, February 19, 2013. Accessed January 13, 2016. http://edition.cnn.com/2013/02/19/opinion/hayden-courage-security-decisions/index.html.

Kennedy, Scott. “Made in China 2025.” Washington, DC: Center for Strategic and International Studies, June 1, 2015. Accessed December 1, 2015. http://csis.org/publication/made-china-2025.

Kirshner, Jonathan. “The Consequences of China’s Economic Rise for Sino-US Relations: Rivalry, Political Conflict, and (Not) War.” In Ross and Zhu, 238-259.

Kissinger, Henry. *On China*. New York: Penguin Press, 2011.

———. *World Order*. New York: Penguin Press, 2014.

Letian Pan, ed. “Ten Features in China’s 11th Five Year Plan.” *People’s Daily*, March 8, 2006. Accessed December 20, 2015. http://www.gov.cn/english/2006-03/08/content_246945.htm.

———. “Abstract of the Eleventh Five-Year Plan Outline (draft).” *People’s Daily*, March 8,

2006. Accessed December 20, 2015. http://www.gov.cn/english/2006-03/08/content_246973.htm.

Lewis, James A. “Cyber War: Definitions, Deterrence, and Foreign Policy.” Statement before the House Committee on Foreign Affairs, September 30, 2015. Accessed January 12, 2016. http://csis.org/files/attachments/ts150930_Lewis.pdf.

Libicki, Martin C. *Crisis and Escalation in Cyberspace.* Santa Monica, CA: RAND, 2012.

Lumbers, Michael. “Whither the Pivot: Alternative US Strategies for Responding to China’s Rise.” *Comparative Strategy* 34, no. 4 (September-October 2015), 311-329. Accessed January 27, 2016. http://dx/doi.org/10.1080/01495933.2015.1069510.

Ma Kai. “The 11th Five-Year Plan: Targets, Paths, and Policy Orientation.” National Development and Reform Commission, March 19, 2006. Accessed December 27, 2015. http://www.gov.cn/english/2006-03/23/content_234832.htm

Mandiant. *APT1: Exposing One of China’s Cyber Espionage Units*. Alexandria, VA: Mandiant, 2013. Accessed November 23, 2015. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

McConnell, Mike, Michael Chertoff, and William Lynn. “China’s Cyber Thievery is National Policy, and it Must Be Challenged.” *Wall Street Journal*, January 27, 2012. Accessed October 2, 2015. http://www.wsj.com/articles/SB10001424052970203718504577178832338032176.

McConnell, Mike. Untitled speech. Bond Lecture Series, University of Missouri, March 12, 2015. Accessed January 8, 2016. https://www.youtube.com/watch?v=_RPT9pAVUsY.

Melton, Oliver. “China’s Five-Year Planning System: Implications for the Reform Agenda.” Prepared statement presented to US-China Economic and Security Review Commission, April 22, 2015. In US-China Economic and Security Review Commission, *China Ahead of the 13th Five-Year Plan*, 42-64.

Monaco, Lisa. “Expanding Our Ability to Combat Cyber Threats.” White House blog, April 1, 2015. Accessed January 20, 2016. https://www.whitehouse.gov/blog/2015/04/01/expanding-our-ability-combat-cyber-threats.

Moody, Andrew. “Dissecting China’s Five-Year Plan.” *The Telegraph*, November 23, 2015. Accessed December 15, 2015. http://www.telegraph.co.uk/sponsored/china-watch/politics/12006280/china-five-year-plan.html.

National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.0*, February 12, 2014. Accessed January 20, 2016. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

Neuffer, John. “Testimony before the US-China Economic and Security Review Commission.” Prepared statement presented to US-China Economic and Security Review Commission, June 15, 2011. In US-China Economic and Security Review Commission, *China’s Five-Year Plan*, 80-86.

Obama, Barack. Executive Order 13636. “Improving Critical Infrastructure Cybersecurity.” *Federal Register* 78, no. 33 (February 12, 2013): 11737-11744.

———. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Washington, DC: The White House, May 2011. Accessed January 13, 2016. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_

strategy_for_cyberspace.pdf.

Office of the National Counterintelligence Executive. *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*. Washington, DC: October 2011. Accessed December 5, 2015. https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

Ponemon Institute. *2015 Cost of Cyber Crime Study: United States*. Traverse City, MI: Ponemon Institute, October 2015. Accessed January 29, 2016. https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5208enw.pdf.

Prasad, Eswar S. "The Path to Sustainable Growth in China." Prepared statement presented to US-China Economic and Security Review Commission, April 22, 2015. In US-China Economic and Security Review Commission, *China Ahead of the 13th Five-Year Plan*, 160-178.

R.,S. "The Economist Explains: Why China's Five-Year Plans are So Important." *The Economist explains* (blog), *Economist*, October 26, 2015. Accessed December 01, 2015. http://www.economist.com/blogs/economist-explains/2015/10/economist-explains-24.

Rogin, Josh. "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History'," *Foreign Policy*, July 9, 2012. Accessed August 12, 2015. http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/?wp_login_redirect=0).

Ross, Robert S., and Zhu Feng, eds. *China's Ascent: Power, Security, and the Future of International Politics*. Ithaca, NY: Cornell University Press, 2008.

Shih, Willy C. "Prepared Statement of Dr. Willy C. Shih." Prepared statement presented to US-China Economic and Security Review Commission, June 15, 2011. In US-China Economic and Security Review Commission, *China's Five-Year Plan*, 28-33.

Sutter, Robert G. *China's Rise in Asia: Promises and Perils.* Lanham, MD: Rowman & Littlefield Publishers, 2005.

Thomas, Timothy. "China's Concept of Military Strategy." *Parameters* 44, no. 4 (Winter 2014-15): 39-48.

Tiezzi, Shannon. "China's Response to the US Cyber Espionage Charges." *The Diplomat*, May 21, 2014. Accessed January 20, 2016. http://thediplomat.com/2014/05/chinas-response-to-the-us-cyber-espionage-charges/.

———. "US, China Hold Cyber Talks Before Xi's Visit." *The Diplomat*, September 15, 2015. Accessed January 13, 2016. http://thediplomat.com/2015/09/us-china-hold-cyber-talks-before-xis-visit/.

US Department of Defense. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013*. Washington, DC: Office of the Secretary of Defense, 2013. Accessed January 14, 2016. http://www.defense.gov/Portals/1/Documents/pubs/2013_China_Report_FINAL.pdf.

US Department of Defense. Defense Science Board. *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*. Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, January 2013. Accessed January 8, 2016. http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

US Department of Homeland Security. *Fact Sheet: EO 13636 Improving Critical Infrastructure Cybersecurity and PPD-21 Critical Infrastructure Security and Resilience,* March 2013. Accessed January 13, 2016. https://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf.

US Department of Homeland Security. Office of Public Affairs. *First US-China High-level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes*, December 2, 2015. Accessed January 25, 2016. http://www.dhs.gov/news/2015/12/02/first-us-china-high-level-joint-dialogue-cybercrime-and-related-issues-summary.

US Department of Justice. Office of Public Affairs. *US Charges Five Chinese Military Hackers for Cyber Espionage Against US Corporations and a Labor Organization for Commercial Advantage*, May 19, 2014. Accessed January 20, 2016. http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

US Government Accountability Office. *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented* (GAO-13-187). Washington, DC: Government Accountability Office, February 2013. Accessed January 14, 2016. http://www.gao.gov/assets/660/652170. pdf.

US-China Economic and Security Review Commission. *2010 Report to Congress of the US-China Economic and Security Review Commission*. 111th Cong., 2d sess., November 2011. Washington, DC: US Government Printing Office, November 2010. Accessed January 15, 2016. http://origin.www.uscc.gov/sites/default/files/annual_reports/2010-Report-to-Congress.pdf.

———. *China Ahead of the 13th Five-Year Plan: Competitiveness and Market Reform: Hearing before the US-China Economic and Security Review Commission.* 114th Cong., 1st sess., April 22, 2015. Accessed December 01, 2015. http://origin.www.uscc.gov/sites/default/files/transcripts/April%2022%2C%202015%20Hearing%20Transcript.pdf.

———. *China's Five-Year Plan, Indigenous Innovation and Technology Transfers and Outsourcing: Hearing before the US-China Economic and Security Review Commission.* 112th Cong., 1st sess., June 15, 2011. Accessed December 3, 2015. http://origin.www.uscc.gov/sites/default/files/transcripts/ 6.15.11HearingTranscript.pdf.

Walters, Riley. "Cyber Attacks on US Companies in 2014," Heritage, Issue Brief #4289, October 27, 2014. Accessed January 20, 2016. http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014#_ftn18.

White House. *Administration Strategy on Mitigating the Theft of US Trade Secrets*. February 2013. Accessed January 22, 2016. https://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_us_trade_secrets.pdf.

———. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,* n.d. [but released on May 29, 2009]. Accessed October 28, 2015. https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

White House. Office of the Press Secretary. *Background Briefing on the Launch of the Cybersecurity Framework*, February 12, 2014. Accessed January 20, 2016. https://www.whitehouse.gov/the-press-office/2014/02/12/background-briefing-launch-cybersecurity-framework.

———. *Fact Sheet: Cybersecurity Legislative Proposal*, May 12, 2011. Accessed January 13, 2016. https://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal.

———. *Fact Sheet: President Xi Jinping's State Visit to the United States*, September 25, 2015. Accessed January 13, 2016. https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

———. *Fact Sheet: The Administration's Cybersecurity Accomplishments*, May 12, 2011. Accessed January 13, 2016. https://www.whitehouse. gov/the-press-office/2011/05/12/fact-sheet-administrations-cybersecurity-accomplishments.

———. *Remarks by the President on Securing Our Nation's Cyber Infrastructure*, May 29, 2009. Accessed January 10, 2016. https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

———. *Remarks by the President in Year-End Press Conference*, December 19, 2014. Accessed January 20, 2016. https://www.whitehouse.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference.

———. *Remarks by the President at the Cybersecurity and Consumer Protection Summit*, February 13, 2015. Accessed January 12, 2016. https://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.

———. *Securing Cyberspace: President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts*, January 13, 2015. Accessed January 12, 2016. https://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat.

———. *Statement by the Press Secretary on the Executive Order Entitled "Imposing Additional Sanctions with Respect to North Korea,"* January 2, 2015. Accessed January 20, 2016. https://www.whitehouse.gov/the-press-office/2015/01/02/statement-press-secretary-executive-order-entitled-imposing-additional-s.

White House. Office of the Press Secretary. State of the Union addresses.

———. *Remarks by the President in State of the Union Address*, January 27, 2010. Accessed January 19, 2016. https://www.whitehouse.gov/the-press-office/remarks-president-state-union-address.

———. *Remarks by the President in State of the Union Address*, January 25, 2011. Accessed January 19, 2016. https://www.whitehouse.gov/the-press-office/2011/01/25/remarks-president-state-union-address.

———. *Remarks by the President in State of the Union Address*, January 24, 2012. Accessed January 19, 2016. https://www.whitehouse.gov/the-press-office/2012/01/24/remarks-president-state-union-address.

———. *Remarks by the President in the State of the Union Address*, February 12, 2013. Accessed January 19, 2016. https://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address.

———. *President Barack Obama's State of the Union Address*, January 28, 2014. Accessed January 19, 2016. https://www.whitehouse.gov/the-press-office/2014/01/28/president-barack-obamas-state-union-address.

———. *Remarks by the President in State of the Union Address*, January 20, 2015. Accessed

January 19, 2016. https://www.whitehouse.gov/the-press-office/2015/01/20/remarks-president-state-union-address-january-20-2015.

———. *Remarks of President Barack Obama—State of the Union Address as Delivered,* January 13, 2016. Accessed March 24, 2016. https://www.whitehouse.gov/the-press-office/2016/01/12/remarks-president-barack-obama-%E2%80%93-prepared-delivery-state-union-address.

Xinhua News Agency. "Xi Pledges 'Great Renewal of Chinese Nation'," Xinhuanet, November 29, 2012. Accessed April 1, 2016. http://news.xinhuanet.com/english/china/2012-11/29/c_132008231.htm.

———. "Xinhua Insight: China's New Five-Year Plan Covers Home Stretch to Prosperity," Xinhuanet, October 30, 2015. Accessed December 15, 2015. http://news.xinhuanet.com/english/2015-10/30/c_134764096.htm.

Zheng Bijian. *China's Peaceful Rise*. Washington, DC: Brookings Institution Press, 2006. Accessed January 4, 2016. ProQuest ebrary.

Zhu Feng. "China's Rise Will Be Peaceful: How Unipolarity Matters." In Ross and Zhu, 34-54.